# DIDSBURY GOOD NEIGHBOURS AND DIDSBURY PAVILION CAFE LTD

*Didsbury Pavilion Cafe Ltd (DPC Ltd) is a wholly-owned subsidiary of Didsbury Good Neighbours (DGN)*
*Registered Charity: 1145943*

## Data Protection Policy

This policy was adopted on

Date: 28/07/2021

Review Date: 28/07/2023

Signed:

Chair of Trustees Sue Thurston

**This is the Data Protection Policy of DIDSBURY GOOD NEIGHBOURS (DGN) and Didsbury Pavilion Cafe Ltd (DPC Ltd)**

## Section A: Scope of this policy
## Section B: Policy statement
## Section C: Guidelines for implementation

**Section A**
**Scope of this policy:**

This policy covers the actions and obligations of DGN's and DPC Ltd's Board

members, trustees, staff and volunteers in relation to the handling of all types of information. This includes information about specific individuals, which is subject to the Data Protection Act 2018 and to other privileged information that may be obtained as a result of a person's role within the organisation.

**Section B**

**Our Statement of general policy is:**

- To comply fully with the Data Protection Act 2018
- To recognise the right of individuals to have their personal information respected and properly maintained.
- To ensure that anyone acting on our behalf complies with the Data Protection Act 2018 and does not breach any part of it. All trustees, staff and volunteers have a general duty of confidentiality. The only exception to this duty is where there is a higher duty of disclosure to safeguard an adult at risk.
- To provide appropriate guidance on responsibilities under the Acts to trustees, staff and, where relevant, volunteers.
- DGN and DPC Ltd are registered with the Information Commissioner's Office (ICO) as organisations which processes personal data and will use the ICO for general guidance on data protection and freedom of information, and will ensure that trustees, staff, and volunteers use the ICO's self- assessment toolkit for small enterprises to support the implementation of this policy.
- To appoint a member of DGN's and DPC Ltd's board to lead on any data protection issues within the charity. Specialist advice can be obtained from the ICO, by phone on 01625 545 745 or email casework@ico.org.uk
- To empower the Chair of Trustees to be the Responsible Person responsible for monitoring our compliance with the Act.
- To implement disciplinary procedures for misuse of personal data.
- To review and revise this policy as necessary, at least every 2 years.

**Section C**

**Guidelines for implementation of the Data Protection Policy**

**1: Introduction**

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR) which relates to how Personal data is used by organisations, businesses or government. This is information about living, identifiable individuals. This need not be particularly sensitive information and can be as little as a name and address.

**The Data Protection Act 2018 works in two ways, by**

- giving individuals (**data subjects**) certain rights
- requiring those who record and use personal information (**data controllers**) to be open about their use of that information and to follow sound and proper practices (the **Data Protection Principles**).

**The Data Controller** can be any type of company, organisation or individual, and need not necessarily own a computer. The size of the organisation is immaterial; the nature of the organisation is unimportant; the amount of personal data held is irrelevant. DGN and DPC Ltd are data controllers. The Chair of Trustees as the Responsible Person, will monitor compliance with the Regulations on behalf of DGN and DPC Ltd.

DGN and DPC Ltd are notifiable organisations under the Data Protection Act 2018. We must comply with the eight Data Protection Principles. The onus is on us, as data controllers, to ensure that use of data by staff, trustees, volunteers or contractors does not breach the Data Protection Principles.

**1a Data Protection Principles**

Under the Act, the data protection principles set out the main responsibilities for organisations and require 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 Act 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.

## 1b Definitions under the Data Protection Act 2018

**Fair processing:** when we collect information from individuals we should be honest and open about why we want it. In addition, we must have a legitimate reason for processing the data. We should explain (inmost cases in writing):

- Who the data controller is (DGN/DPC Ltd)
- What we intend to use the information for
- To whom we intend to give the personal data.
- If we use, or intend to use, personal data for direct marketing purposes, we should ensure that data subjects are made aware of this and given an opportunity not to have their particular data processed for this purpose.

**Adequate, relevant and not excessive:** data users (our staff/board members/trustees/volunteers) should monitor the quantities of data held for their purposes and ensure that they hold neither too much nor too little data in respect of the individuals about whom their data is held. We must only hold the data that we actually need.

**Accurate:** personal data must be accurate and any errors must be corrected or removed and reviewed regularly (every six months).

**No longer than necessary:** only in exceptional circumstances should data be kept indefinitely. We should have a system for the removal of different categories of data from our system after certain periods.

**Security: Data must be kept secure at all times,** taking into account the nature of the data, and the harm to the data subject which could arise from disclosure or loss of data.

**Authorised access to data and computer records:** only people who are authorised can gain access to personal data. Authorisation is as below:

Chair of Trustees (Responsible Person) – all data
Nominated DGN Data Protection Trustee -all DGN data
Nominated DPC Ltd Board Member- all DPC Ltd data
DGN Treasurer – data relating to DGN payroll and all finance data and monitoring data
DPC Ltd Treasurer – data relating to DPC Ltd payroll and all finance data and monitoring data
DGN Trustee representatives on Finance and Audit committee – all DGN finance data
DPC Ltd Board members – all DPC Ltd finance data
DGN Trustee representatives on DGN Operations Committees – all DGN service user, volunteer and HR data.

DGN Manager – all DGN Data
DGN Volunteer Coordinator – all DGN volunteer and service user data
DGN Activity and Events Coordinator – all DGN volunteer and service user data and maintenance of the Charity's DBS register
DPC Ltd Cafe Manager- All DPC Ltd data
Didsbury Neighbourhood Centre Business Manager -all lettings and building data

Misuse of personal data by trustees or members of staff will be a disciplinary offence.

**Access to records by individuals other than staff:**

We will specify those types of individual and organisation to whom personal data can be disclosed. Particular attention should be given to:

a) the siting of computer terminals so as to prevent casual callers to premises being able to read personal data on screen (this is particularly important in the case of the shared laptop used in the cafe area. Care should also be taken when using laptop computers to access DGN data in the Neighbourhood Centre offices and when away from DGN and DPC Ltd premises (e.g. working from home) .
b) Procedures to verify the identify of callers (especially telephone callers) seeking information held on computer.

**Prevention of the accidental loss or theft of personal data**: Attention must be given to unforeseen contingencies such as the theft of computer equipment or fire.

a) We will keep all of our data on DGN and DPC Ltd owned equipment and back up copies of files in secure areas away from such equipment.
b) We will ensure the physical security of all equipment.
c) Personal equipment must not be used for collection or storage of any DGN or DPC Ltd data without prior approval of the Board.

**Sensitive Data**

There are eight categories of sensitive personal data:

1 the racial or ethnic origin of data subjects
2 their political opinions
3 their religious beliefs or other beliefs of a similar nature
4 membership of trade unions
5 physical health, mental health or condition
6 their sexual life or sexual orientation
7 genetic data
8 biometric data

If ***any*** such information is held we will need the explicit consent of the individual

concerned and security procedures will have to be adequate for the protection of sensitive data.

**Conditions for Processing**

In addition to complying with all six data protection principles when processing personal data a data controller must also satisfy at least one processing condition. The processing conditions are:

a) **Consent** - data subjects must be offered real choice and control and must explicitly consent to their data being processed for specific reasons.

b) **Contract- processing must be necessary to deliver a contractual service to someone or because they have asked you to do something before entering into a contract (**e.g. provide a quote).

c) **Legal Obligation –** processing must be necessary to comply with a common law or statutory obligation.

d) **Vital interests –** processing must be necessary to protect a data subject or another person and the data subject must be incapable of giving consent

e) **Public Task-** processing must be necessary ' to carry out a task in the exercise of official authority' e.g. public functions and powers that are set out in law; or to perform a specific task in the public interest that is set out in law.

f) **Legitimate interests** - processing must be appropriate where people's data is used in ways they would reasonably expect and which has a minimal privacy impact, or where there is a compelling justification for the processing.

**Manual Data**

Such records need not be notified to the Commissioner, but should be handled in accordance with data protection principles. Manual records are covered by the Act if they form part of any relevant filing system defined as "*any set of information relating to individuals and structured, either by reference to criteria relating to individuals, or in such a way that specific information relating to a particular individual is readily accessible*". (i.e. If we can search the records for information on an individual, the system is a relevant one.)

**Compensation**

**I**ndividuals may seek compensation through the courts if they have suffered damage because of any contravention of the Regulations.

**Subject access requests**

Must be dealt with promptly and certainly within 28 days of the date of receipt. In response to a request, individuals are entitled to a copy of the information held about them, both on computer and as part of a relevant filing system. They also have the right to receive a description of why their information is processed, anyone it may be disclosed to, and any information available about the source of the data. It is important that staff know how to recognise a subject access request and realise that it must be dealt with urgently.

**The right to be forgotten**

The Act introduces a right for individuals to have personal data erased.

The right to erasure is also known as 'the right to be forgotten'.

Individuals can make a request for erasure verbally or in writing.

We have one month to respond to a request.

The right is not absolute and only applies in certain circumstances.

This right is not the only way in which the Act places an obligation on us to consider whether to delete personal data.

**Dealing with direct marketing suppression requests**

individuals have the right not to have their personal data processed for direct marketing purposes*. When collecting data, we should give people the opportunity to let us know whether or not they wish to receive marketing material from us*. If they do not, or if we do not ask this question, we must ensure that we can suppress their details on any mailing lists we use. If it is intended to share information for direct marketing purposes we must first check with the individuals concerned if they are happy for us to do this. This should be done when we first collect the data, perhaps on our application/registration form. We must not pass on the details of anyone who says that they object to their details being used in this way. If we have not previously sent out marketing material or passed on details to third parties for marketing, we should obtain the consent of existing members/service users before beginning to process their data for these purposes.

**1c What Sort of Records?**

In DGN and DPC Ltd's case, the sort of records we hold include:

- Personnel information, relating to existing or past employees, including payroll and sickness information
- Current or past volunteer records
- Membership/service user details
- Contact and PR lists

- Funders, donors
- CCTV images

- All Board members, trustees and staff must consider whether information they hold (paper or electronic) falls within the definition of the Regulations and draw up appropriate guidelines for inclusion in this Policy, we will use the ICO's self- assessment toolkit for small enterprises.

## 1d Record Keeping and Disposal

**Introduction**

We will collect and store only data which enables us to operate and will maintain a register of all of the systems or contexts in which we process data. When data becomes out of date and of no further use, it will be removed and destroyed (shredded). We will set review and retention periods on all documents. Our manual personnel and payroll records will be kept in a locked filing cabinet, with keys held by the authorised people listed in section 1 b of this policy. Personnel information held on computer (such as letters) will be password protected and deleted once their immediate use has passed and a paper copy (where required) has been filed. DGN's computer hard drives must be wiped before disposal of the computers

References

Confidential employment references *given by* DGN and DPC Ltd are exempt from the right of access provisions of the Regulation. For practical reasons, it is sensible not to keep copies of such references in the employee's file.

References *received by* DGN and DPC Ltd are not exempt, provided that the identity of a third party is not divulged without permission (e.g. the author). The spirit of the Regulations is about openness and the Guidance from the ICO is that, if possible, a copy of the reference should be provided but with information about third parties removed if it is not practical to gain their consent. In future, when requesting references, DGN and DPC Ltd could consider whether to inform referees that the subject of the reference will be entitled to have access to it.

Both successful and unsuccessful job applicants also have the right of access to application forms, interview notes, test results etc, retained in a recruitment file by the employer or by the recruitment agency. In principle, the records should be destroyed once the purpose for keeping them no longer exists, i.e. when all the decisions have been taken and the campaign is over. However, this must be balanced against the possible need to defend the decisions against a claim of discrimination.

**Working Time Regulations 1998**

Adequate records must be kept to demonstrate compliance with the average weekly and night time working limits. In DGN and DPC Ltd's case these are monitored through the staff Rotas, TOIL, and Holiday sheets monitored by line managers and DGN's Treasurer/DPC Ltd Board.

**Pay-roll related Records**

Enough information must be retained to complete in full the year-end returns. Where employment is contracted out, records should be kept for the entire duration for the employment, and for three years after that.

**Disposal**

The Data Protection Act 2018 places an obligation on us to dispose of personal information when it is no longer needed. To prevent unauthorised or accidental disclosure of the information, it is important to exercise care in its disposal, including protecting its security and confidentiality during storage, transportation, handling and destruction. All staff have a responsibility to consider safety and security when disposing of personal information in the course of their work – such information should be shredded if on paper and permanently deleted from computer hard drives.

The ensuing chart summarises the legal requirements associated with certain kinds of information. When deciding on retention times, we have considered the following **in order**:

**i)** any legal requirements (e.g. possible negligence action);
**ii)** The length of any appeals procedure relating to the information
**iii)** The number of times in the last two or three years that you have had to refer to a particular type of record (if the answer is never, then get rid of it)

We will keep disposal records , indicating what records have been destroyed, when, by whom, and using what method of destruction. Records which have been kept or archived will also be tracked. The record will be part of an electronic records management system; The disposal record applies to both paper and electronic records. It will not, in itself, contain personal information (e.g. names). It will include the date and manner of disposal.