1. Information Security BNENC GDPR) Policy Practice & Procedures

a. Breckfield & North Everton Neighbourhood Council will maintain its registration under the Data Protection Act and any subsequent legislation which may be enforced
b. Copies of clients' and/or employees' details will not be forwarded to any agency without prior consent of those concerned and by agreement with the Director
c. Clients' and/or employees' personal details will not be disclosed to any third party, unless in the case of an employment reference, and only then if the request is made in writing
d. Clients and employees will have full rights to see information which is held on their personal file and on the computer. This information must only be accessed in the presence of a Breckfield & North Everton Neighbourhood Council staff member
e. Every employee should abide by the principles of the Data Protection Act 1984 (updated 1999) which are:

    - Personal Data should be obtained fairly and lawfully.
    - It should be held for the purpose(s) given in the registration.
    - It should not be used or disclosed in a way incompatible with the purpose(s) in the registration.
    - It should be adequate, relevant and not excessive for the purpose(s).
    - It should be accurate and, where necessary, kept up to date.
    - It should be kept for no longer than necessary.
    - It should be available to the 'data subject'.
    - It should be kept securely.

f. Client and employee confidentiality will be respected at all times. Should any client and/or employee have cause for concern they should do so in writing to the Chief Officer at Breckfield & North Everton Neighbourhood Council.

13. Controlling Physical Security

Breckfield & North Everton Neighbourhood Council is committed to restricting access to the office, desks, storage areas, equipment and other facilities where unauthorised access by people could compromise security.

To facilitate this, the following principles will be adhered to:

a. Access to the offices is controlled and restricted at all times. Only those who are either known to Breckfield & North Everton Neighbourhood Council, or who have an appointment with Breckfield & North Everton Neighbourhood Council, will be allowed entry.
b. The office will be secured after hours, and during the day if it is unoccupied
c. No clients or visitors will be allowed access to the office area, unless a member of staff is present

14. Controlling Access to Information

a. Each computer in the office is protected with a password which is known only to members of staff. Clients or visitors wishing to use any computer in the office will only be allowed to do so in the presence of a staff member

b. Any printed material containing information taken from personal data will be put through a shredding machine.

15. Staff Training

Employees are made aware of information security issues during their induction. Any violation of the security policy may lead to disciplinary action.

16. General Data Protection Regulations Privacy Notice

We issue this privacy notice in the interests of transparency over how we use the personal data that we collect from job applicants/employees.

Personal data for these purposes means any information relating to an identified or identifiable person.

"**Sensitive personal data**" means personal data consisting of information as to -

a) the racial or ethnic origin of the individual,

b) their political opinions,

c) their religious or philosophical beliefs,

d) their membership of a trade union,

e) their physical or mental health or condition,

f) their sexual life,

g) the commission or alleged commission by them of any offence,

h) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings,

i) genetic data; and

j) biometric data where processed to uniquely identify a person (for example a photo in an electronic passport)

Data Controller

For data protection purposes the "**data controller**" means the person or organisation who determines the purposes for which and the manner in which any personal data are processed.

The data controller is Paul Robinson, Director of Operations, Breckfield & North Everton Council Ltd, The Breckfield Centre, Breckfield Road North, Liverpool L5 4QT

Purpose of processing the data

It is necessary for us to process personal data of both job applicants and employees for the following reasons:

1. We will need the information in order to identify the individual for the purposes of recruitment;
2. We will need to maintain that information for the general purposes of the ongoing employment relationship including performing the employment contract and maintaining the health and safety of individuals on our premises.

Our legal basis for processing personal data of applicants and staff is that:

1. Processing the personal data is necessary for the purpose of carrying out the employment contract or to take steps to enter into an employment contract;
2. Processing is necessary to comply with a legal obligation (for example we are obliged under employment law to include in a written statement of employment terms the identity of the parties to the employment contract);
3. Processing the data is necessary to protect the vital interests of an individual (for example we are legally responsible for the health and safety of staff and job applicants (when they are on our premises) and so it is necessary to process data relating to those individuals for that reason); and/or
4. Processing the data is necessary for the purposes of our "**legitimate interests**" as the data controller (except where such interests are overridden by the interests, rights or freedoms of the individual).

Our "legitimate interests" for these purposes are:

1. the need to process data on applicants and staff for the purposes of assessing suitability for employment and then carrying out the employment contract;
2. the need to gather data for the purposes safeguarding the health and safety of job applicants and employees;
3. the need to transfer employee data intra-group for administrative purposes; and
4. the need to process employee data for the purposes of ensuring network and information security.

We may from time to time need to process sensitive personal data, for example medical records or other information relating to the health and well-being of an individual.

In that case we will either obtain the explicit consent of the individual to the processing of such data or we may consider the processing of that data as being necessary for carrying out our obligations as an employer. That will be assessed on a case by case basis.

There is no strict statutory or contractual requirement for you to provide data to us but if you do not provide at least that data that is necessary for us to assess suitability for employment and then to conduct the employment relationship then it will not practically be possible for us to employ you.

Recipients of personal data

Your personal data may be received by the following categories of people:

1. Our HR department;
2. In the case of job applicants, the interviewer and prospective manager;
3. Any individual authorised by us to maintain personnel files;
4. Our professional advisers; and
5. Appropriate external regulators and authorities (such as HMRC and HSE)

We do not envisage that your data would be transferred to a third country. If we perceive the need to do that we would discuss that with you and explain the legal basis for the transfer of the data at that stage.

Duration of storage of personal data

We will keep personal data for no longer than is strictly necessary, having regard to the original purpose for which the data was processed. In some cases we will be legally obliged to keep your data for a set period. Examples are below:

Income tax and NI returns, income tax records and correspondence with HMRC: We are obliged to keep these records for not less than 3 years after the end of the financial year to which they relate.

Wage and salary records: We are obliged to keep these records for 6 years.

Your rights in relation to your personal data

1. <u>The right to be forgotten</u>

You have the right to request that your personal data is deleted if:

a) it is no longer necessary for us to store that data having regard to the purposes for which it was originally collected; or
b) in circumstances where we rely solely on your consent to process the data (and have no other legal basis for processing the data), you withdraw your consent to the data being processed; or

c) you object to the processing of the data for good reasons which are not overridden by another compelling reason for us to retain the data; or
d) the data was unlawfully processed; or
e) the data needs to be deleted to comply with a legal obligation.

However, we can refuse to comply with a request to delete your personal data where we process that data:

a) to exercise the right of freedom of expression and information;
b) to comply with a legal obligation or the performance of a public interest task or exercise of official authority;
c) for pubic health purposes in the public interest;
d) for archiving purposes in the public interest, scientific research, historical research or statistical purposes; or
e) the exercise or defence of legal claims.

2. The right to data portability

You have the right to receive the personal data which you have provided to us, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided (us) where:

a) the processing is based on consent or on a contract; and
b) the processing is carried out by automated means.

Note that this right only applies if the processing is carried out by "automated means" which means it will not apply to most paper based data.

3. The right to withdraw consent

Where we process your personal data in reliance on your consent to that processing, you have the right to withdraw that consent at any time. You may do this in writing to the HR team or to your line manager.

4. The right to object to processing

Where we process your personal data for the performance of a legal task or in view of our legitimate interests you have the right to object on "grounds relating to your particular situation". If you wish to object to the processing of your personal data you should do so in writing to HR or to your line manager stating the reasons for your objection.

Where you exercise your right to object we must stop processing the personal data unless:

- we can demonstrate compelling legitimate grounds for the processing, which override your interests, rights and freedoms; or

- the processing is for the establishment, exercise or defence of legal claims.

5. The right of subject access

   So that you are aware of the personal data we hold on you, you have the right to request access to that data. This is sometimes referred to as making a "subject access request".

6. The right to rectification

   If any of the personal data we hold on you is inaccurate or incomplete, you have the right to have any errors rectified.

   Where we do not take action in response to a request for rectification you have the right to complain about that to the Information Commissioner's Office.

7. The right to restrict processing

   In certain prescribed circumstances, such as where you have contested the accuracy of the personal data we hold on you, you have the right to block or suppress the further processing of your personal data.

8. Rights related to automated decision making and profiling

   The GDPR defines "profiling" as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict:

   - performance at work;
   - economic situation;
   - health;
   - personal preferences;
   - reliability;
   - behaviour;
   - location; or
   - movement

You have the right not to be subject to a decision when it is based on automated processing; and it produces a legal effect or a similarly significant effect on you.

However, that right does not apply where the decision is necessary for purposes of the performance of a contract between you and us. We may use data related to your performance or attendance record to make a decision as to whether to take

disciplinary action. We consider that to be necessary for the purposes of conducting the employment contract. In any event that is unlikely to be an automated decision in that action will not normally be taken without an appropriate manager discussing the matter with you first and then deciding whether the data reveals information such that formal action needs to be taken. In other words there will be “human intervention” for the purposes of the GDPR and you will have the chance to express your point of view, have the decision explained to you and an opportunity to challenge it.

Complaints

Where you take the view that your personal data are processed in a way that does not comply with the GDPR, you have a specific right to lodge a complaint with the relevant supervisory authority. The supervisory authority will then inform you of the progress and outcome of your complaint. The supervisory authority in the UK is the ICO.