GDPR Policy

Version : 1

Confidentiality Policy	**Chief Executive Officer**
Review Date	**October 2024**
Frequency of review	**This policy must be reviewed every 3 years or as deemed necessary**
File Location	**BOT – Policy**
Signed	**G Day**

A) INTRODUCTION

We may have to collect and use information about people with whom we work. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We will ensure that we treat personal information lawfully and correctly.

To this end we fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR).

This policy applies to the processing of personal data in manual and electronic records kept by us in connection with our human resources function as described below. It also covers our response to any data breach and other rights under the GDPR.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

B) DEFINITIONS

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

C) DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a) processing will be fair, lawful and transparent
b) data be collected for specific, explicit, and legitimate purposes
c) data collected will be adequate, relevant and limited to what is necessary for the purposes of processing
d) data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
e) data is not kept for longer than is necessary for its given purpose
f) data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
g) we will comply with the relevant GDPR procedures for international transferring of personal data

D) TYPES OF DATA HELD

We keep several categories of personal data on our employees in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the data within our computer systems, for example, our holiday booking system.

Specifically, we hold the following types of data:

a) personal details such as name, address, phone numbers
b) information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter, references from former employers, details on your education and employment history etc.
c) details relating to pay administration such as National Insurance numbers, bank account details and tax codes
d) medical or health information
e) information relating to your employment with us, including:

    i) job title and job descriptions
    ii) your salary
    iii) your wider terms and conditions of employment
    iv) details of formal and informal proceedings involving you such as letters of concern, disciplinary and grievance proceedings, your annual leave records, appraisal and performance information
    v) internal and external training modules undertaken

All of the above information is required for our processing activities. More information on those processing activities are included in our privacy notice for employees, which is available from your manager.

E) EMPLOYEE RIGHTS

You have the following rights in relation to the personal data we hold on you:

a) the right to be informed about the data we hold on you and what we do with it;
b) the right of access to the data we hold on you. More information on this can be found in the section headed "Access to Data" below and in our separate policy on Subject Access Requests";
c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
d) the right to have data deleted in certain circumstances. This is also known as 'erasure';
e) the right to restrict the processing of the data;
f) the right to transfer the data we hold on you to another party. This is also known as 'portability';
g) the right to object to the inclusion of any information;
h) the right to regulate any automated decision-making and profiling of personal data.

More information can be found on each of these rights in our separate policy on employee rights under GDPR.

F) RESPONSIBILITIES

In order to protect the personal data of relevant individuals, those within our business who must process data as part of their role have been made aware of our policies on data protection.

We have also appointed employees with responsibility for reviewing and auditing our data protection systems.

G) LAWFUL BASES OF PROCESSING

We acknowledge that processing may be only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.

Where no other lawful basis applies, we may seek to rely on the employee's consent in order to process data.

However, we recognise the high standard attached to its use. We understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate. Employees will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

H) ACCESS TO DATA

As stated above, employees have a right to access the personal data that we hold on them. To exercise this right, employees should make a Subject Access Request. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request. In these circumstances, a reasonable charge will be applied.

Further information on making a subject access request is contained in our Subject Access Request policy.

I) DATA DISCLOSURES

The Organisation may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

a) any employee benefits operated by third parties;
b) disabled individuals - whether any reasonable adjustments are required to assist them at work;
c) individuals' health data - to comply with health and safety or occupational health obligations towards the employee;
d) for Statutory Sick Pay purposes;

e) HR management and administration - to consider how an individual's health affects his or her ability to do their job;
f) the smooth operation of any employee insurance policies or pension plans;
g) to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty.

These kinds of disclosures will only be made when strictly necessary for the purpose.

J) DATA SECURITY

All our employees are aware that hard copy personal information should be kept in a locked filing cabinet, drawer, or safe.

Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so that are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops etc. when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Employees must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it should be protected by:

a) ensuring that data is recorded on such devices only where absolutely necessary.
b) using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted.
c) ensuring that laptops or USB drives are not left where they can be stolen.

Failure to follow the Organisation's rules on data security may be dealt with via the Organisation's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

K) THIRD PARTY PROCESSING

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain the Organisation's commitment to protecting data.

L) INTERNATIONAL DATA TRANSFERS

The Organisation does not transfer personal data to any recipients outside of the EEA.

M) REQUIREMENT TO NOTIFY BREACHES

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

More information on breach notification is available in our Breach Notification policy.

N) TRAINING

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/protection officers for the Organisation are trained appropriately in their roles under the GDPR.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Organisation of any potential lapses and breaches of the Organisation's policies and procedures.

O) RECORDS

The Organisation keeps records of its processing activities including the purpose for the processing and retention periods in its HR Data Record. These records will be kept up to date so that they reflect current processing activities.

P) DATA PROTECTION COMPLIANCE

Our appointed compliance officer in respect of our data protection activities is:

Chief Executive Contact via Disability Action Haringey office.

COMMUNICATIONS POLICY

A) INTRODUCTION

1) IT and Communication plays an essential role in the conduct of our business. The IT infrastructure including e-mail and internet access have therefore significantly improved business operations and efficiencies.

2) How you communicate with people not only reflects on you as an individual but also on us as a business. As a result of this the organisation values your ability to communicate with colleagues, clients/customers and business contacts but we must also ensure that such systems and access are managed correctly, not abused in how they are used or what they are used for.

3) This policy applies to all members of the Organisation who use our or our clients' communications facilities, whether Directors/Consultants, full or part-time employees, contract staff or temporary staff. The parameters and restrictions are outlined below and you are required to read them carefully.

B) GENERAL PRINCIPLES

1) You must use our and our clients' information technology and communications facilities sensibly, professionally, lawfully, consistently with your duties and in accordance with this policy and other Organisation rules and procedures.

2) At all times employees must behave with honesty and integrity and respect the rights and privacy of others in relation to electronic communication and information. The organisation reserves the right to maintain all electronic communication and files.

3) Every employee will be given access to the Intranet and/or Internet as appropriate to their job needs. For those who do not have daily PC access occasional access will be arranged, as necessary, by Management,

4) All PC/network access will be through passwords, and no individual is permitted onto the system using another employee's password. Employees are not permitted to share their password with anyone inside or outside the organisation. Individuals will be allowed to set their own passwords, and must change them as frequently as requested by the system set-up requirements.

5) All information relating to our clients/customers and our business operations is confidential. You must treat our paper-based and electronic information with utmost care.

6) Many aspects of communication are protected by intellectual property rights which can be infringed in a number of ways. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or of other intellectual property rights.

7) Particular care must be taken when using e-mail as a means of communication because all expressions of fact, intention and opinion in an e-mail may bind you and/or the Organisation and can be produced in court in the same way as other kinds of written statements.

8) If you are speaking with someone face to face, via the telephone, in writing via whatever medium you are a representative of the Organisation. Whilst in this role you should not express any personal opinion that you know or suspect might be contrary to the opinions of the Directors or Organisation policy.

9) You must not use any of our or our clients' media to do or say anything which would be subject to disciplinary or legal action in any other context such as sending any sexist, racist, defamatory or other unlawful material. If you are in doubt about a course of action, take advice from a member of management.

C) USE OF ELECTRONIC MAIL

1) **Business use**

Always use the "Bcc" box when mailing to groups whenever the members of the group are unaware of the identity of all the others (as in the case of marketing mailing lists), or where you judge that the membership of the group of one or more individuals should perhaps not be disclosed to the others (as in the case of members of a staff benefit scheme), because if you use the "Cc" box each recipient is informed of the identity (and in the case of external recipients, the address) of all the others. Such a disclosure may breach any duty of confidence owed to each recipient, breach the Organisation's obligations under the General Data Protection Regulation and Data Protection Act or may inadvertently disclose confidential business information such as a marketing list. This applies to both external and internal e-mail.

Expressly agree with the customer/client that the use of e-mail is an acceptable form of communication bearing in mind that if the material is confidential, privileged or commercially sensitive then un-encrypted e-mail is not secure.

If you have sent an important document, always telephone to confirm that the e-mail has been received and read.

In light of the security risks inherent in web-based e-mail accounts, you must not e-mail business documents to your personal web-based accounts. You may send documents to a customer's/clients web-based account if you have the customer's/clients express written permission to do so. However, under no circumstances should you send sensitive or highly confidential documents to a customer's/client's personal web-based e-mail account (e.g. Yahoo, or Hotmail), even if the customer/client asks you to do so.

2) **Personal use**

a) Although our e-mail facilities are provided for the purposes of our business, we accept that you may occasionally want to use them for your own personal purposes. This is permitted on condition that all the procedures and rules set out in this policy are complied with. Be aware, however, that if you choose to make use of our facilities for personal correspondence, the Organisation may need to monitor communications for the reasons shown below.

b) Under no circumstances may the organisation's facilities be used in connection with the operation or management of any business other than that of the Organisation or a customer/client of the Organisation unless express permission has been obtained from a member of management.

c) You must ensure that your personal e-mail use:

- does not interfere with the performance of your duties;
- does not take priority over your work responsibilities;
- does not cause unwarranted expense or liability to be incurred by the Organisation or our clients;
- does not have a negative impact on our business in any way; and
- is lawful and complies with this policy.

d) The Organisation will not tolerate the use of the E-mail system for unofficial or inappropriate purposes, including:

(i) any messages that could constitute bullying, harassment or other detriment;

(ii) on-line gambling;

(iii) accessing or transmitting pornography;

(iv) transmitting copyright information and/or any software available to the user; or

(v) posting confidential information about other employees, the Organisation or its customers or suppliers.

D) USE OF INTERNET AND INTRANET

1) We trust you to use the internet sensibly. Although internet facilities are provided for the purposes of our business, we accept that you may occasionally want to use them for your own personal purposes. This is permitted on condition that all the procedures and rules set out in this policy are complied with and your use of the internet does not interfere in any way with the performance of your duties.

2) Whenever you access a web site, you should always comply with the terms and conditions governing its use. Care must be taken in the use of information accessed through the Internet. Most information is unregulated, and as such there is no guarantee of accuracy.

3) The use of the Internet to access and/or distribute any kind of offensive material, or material that is not work-related, leaves an individual liable to disciplinary action which could lead to dismissal.

4) You must not:

   a) use any images, text or material which are copyright-protected, other than in accordance with the terms of the license under which you were permitted to download them;

   b) introduce packet-sniffing or password-detecting software;

   c) seek to gain access to restricted areas of the Organisation's network;

   d) access or try to access data which you know or ought to know is confidential;

   e) introduce any form of computer virus; nor

   f) carry out any hacking activities.

E) VIRUS PROTECTION PROCEDURES

In order to prevent the introduction of virus contamination into the software system the following must be observed:-

a) unauthorised software including public domain software, magazine cover disks/CDs or Internet/World Wide Web downloads must not be used; and

b) all software must be virus checked using standard testing procedures before being used.

F) USE OF COMPUTER EQUIPMENT

In order to control the use of the Organisation's computer equipment and reduce the risk of contamination the following will apply:

a) The introduction of new software must first of all be checked and authorised by a member of management or a client's nominated senior member of management before general use will be permitted.

b) Only authorised staff should have access to the Organisation's computer equipment.

c) Only authorised software may be used on any of the Organisation's computer equipment.

d) Only software that is used for business applications may be used.

e) No software may be brought onto or taken from the Organisation's premises without prior authorisation.

f) Unauthorised access to the computer facility will result in disciplinary action.

g) Unauthorised copying and/or removal of computer equipment/software will result in disciplinary action, such actions could lead to dismissal.

G) SYSTEM SECURITY

1) Security of our or our clients' IT systems is of paramount importance. We owe a duty to all of our customers/clients to ensure that all of our business transactions are kept confidential. If at any time we need to rely in court on any information which has been stored or processed using our IT systems it is essential that we are able to demonstrate the integrity of those systems. Every time you use the system you take responsibility for the security implications of what you are doing.

2) The Organisation's system or equipment must not be used in any way which may cause damage, or overloading or which may affect its performance or that of the internal or external network.

3) Keep all confidential information secure, use it only for the purposes intended and do not disclose it to any unauthorised third party.

H) WORKING REMOTELY

1) This part of the policy and the procedures in it apply to your use of our systems, to your use of our laptops, and also to your use of your own computer equipment or other computer equipment (e.g. client's equipment) whenever you are working on Organisation business away from our premises (working remotely).

2) When you are working remotely you must:

a) password protect any work which relates to our business so that no other person can access your work;

b) position yourself so that your work cannot be overlooked by any other person;

c) take reasonable precautions to safeguard the security of our laptop computers and any computer equipment on which you do Organisation business, and keep your passwords secret;

d) inform the police and the Organisation as soon as possible if either a Organisation laptop in your possession or any computer equipment on which you do our work has been stolen; and

e) ensure that any work which you do remotely is saved on the Organisation system or is transferred to our system as soon as reasonably practicable.

3) PDAs or similar hand-held devices are easily stolen and not very secure so you must password-protect access to any such devices used by you on which is stored any personal data of which the Organisation is a data controller or any information relating our business, our clients or their business.

I) PERSONAL TELEPHONE CALLS/ MOBILE PHONES

1) Telephones are essential for our business. Incoming/outgoing personal telephone calls are allowed at the Organisation's office but should be kept to a minimum. We reserve the right to recharge for excessive personal use. When visiting or working on client premises you should always seek permission before using our clients' telephone facilities.

J) MONITORING OF COMMUNICATIONS BY THE ORGANISATION

1) The Organisation is ultimately responsible for all business communications but subject to that will, so far as possible and appropriate, respect your privacy and autonomy. The Organisation may monitor your business communications for reasons which include:

a) providing evidence of business transactions;

b) ensuring that our business procedures, policies and contracts with staff are adhered to;

c) complying with any legal obligations;

d) monitoring standards of service, staff performance, and for staff training;

e) preventing or detecting unauthorised use of our communications systems or criminal activities; and

f) maintaining the effective operation of Organisation communication systems.

2) From time to time the Organisation may monitor telephone, e-mail and internet traffic data (i.e. sender, receiver, subject; non-business attachments to e-mail, numbers called and duration of calls; domain names of web sites visited, duration of visits, and non-business files downloaded from the internet) at a network level (but covering both personal and business communications). This includes monitoring of any additional accounts you may be requested to set up for the purposes of performing your work tasks,

which are subject to the same rules as your work email account. Information acquired through such monitoring may be used as evidence in disciplinary proceedings.

3) Sometimes it is necessary for us to access your business communications during your absence, such as when you are away because you are ill or while you are on holiday.

K) DATA PROTECTION

1) As an employee using our communications facilities, you will inevitably be involved in processing personal data for the Organisation as part of your job. Data protection is about the privacy of individuals, and is governed by the General Data Protection Regulation and current Data Protection Act.

2) Whenever and wherever you are processing personal data for the Organisation you must keep this secret, confidential and secure, and you must take particular care not to disclose such data to any other person (whether inside or outside the Organisation) unless authorised to do so. Do not use any such personal data except as authorised by us for the purposes of your job. If in doubt ask a member of management.

3) The Act gives every individual the right to see all the information which any data controller holds about them. Bear this in mind when recording personal opinions about someone, whether in an e-mail or otherwise. It is another reason why personal remarks and opinions made should be given responsibly, must be relevant and appropriate as well as accurate and justifiable.

4) For your information, the Act provides that it is a criminal offence to obtain or disclose personal data without the consent of the data controller. "Obtaining" here includes the gathering of personal data by employees at work without the authorisation of the employer. You may be committing this offence if without authority of the Organisation: you exceed your authority in collecting personal data; you access personal data held by us; or you pass them on to someone else (whether inside or outside the Organisation).

L) USE OF SOCIAL NETWORKING SITES

Any work related issue or material that could identify an individual who is a customer/client or work colleague, which could adversely affect the organisation a customer/client or our relationship with any customer/client must not be placed on a social networking site. This means that work related matters must not be placed on any such site at any time either during or outside of working hours and includes access via any computer equipment, mobile phone or PDA.

M) CONFIDENTIALITY

Employees are not permitted to register with sites or electronic services in the organisation's name without the prior permission of the Chief executive. They are not permitted to reveal internal organisation information to any sites, be it confidential or otherwise, or comment on organisation matters, even if this is during after-hours or personal use. The organisation confidentiality policy applies to all electronic communication and data.

N) COMPLIANCE WITH THIS POLICY

1) Failure to comply with this policy may result in disciplinary action being taken against you. If there is anything in this policy that you do not understand, please discuss it with a member of management.

2) Please note that the procedures and policies outlined in this policy, and in any related policy, may be reviewed or changed at any time.

POLICY ON YOUR RIGHTS IN RELATION TO YOUR DATA

A) AIM

This policy outlines the rights that data subjects have, under the General Data Protection Regulation (GDPR), in relation to the data about them that we hold. Data subjects, for the purposes of this policy, includes employees (current, prospective and former), workers and contractors.

B) THE RIGHT TO BE INFORMED

In order to keep you informed about how we use your data, we have a privacy notice for employees. You can obtain a copy of the privacy notice from your manager.

The organisation also has a separate privacy notice applicable to job applicants, available from your Chief executive.

You will not be charged for receiving our privacy notices.

Our privacy notices set out:

a) the types of data we hold and the reason for processing the data;
b) our legitimate interest for processing it;
c) details of who your data is disclosed to and why, including transfers to other countries. Where data is transferred to other counties, the safeguards used to keep your data secure are explained;

d) how long we keep your data for, or how we determine how long to keep your data for;
e) where your data comes from;
f) your rights as a data subject;
g) your absolute right to withdraw consent for processing data where consent has been provided and no other lawful reason for processing your data applies;
h) your right to make a complaint to the Information Commissioner if you think your rights have been breached;
i) whether we use automated decision making and if so, how the decisions are made, what this means for you and what could happen as a result of the process;
j) the name and contact details of our data protection officer.

C) THE RIGHT OF ACCESS

You have the right to access your personal data which is held by us. You can find out more about how to request access to your data by reading our Subject Access Request policy.

D) THE RIGHT TO 'CORRECTION'

If you discover that the data we hold about you is incorrect or incomplete, you have the right to have the data corrected. If you wish to have your data corrected, you should complete the Data Correction Form.

Usually, we will comply with a request to rectify data within one month unless the request is particularly complex in which case we may write to you to inform you we require an extension to the normal timescale. The maximum extension period is two months.

You will be informed if we decide not to take any action as a result of the request. In these circumstances, you are able to complain to the Information Commissioner and have access to a judicial remedy.

Third parties to whom the data was disclosed will be informed of the rectification.

E) THE RIGHT OF 'ERASURE'

In certain circumstances, we are required to delete the data we hold on you. Those circumstances are:

a) where it is no longer necessary for us to keep the data;

b) where we relied on your consent to process the data and you subsequently withdraw that consent. Where this happens, we will consider whether another legal basis applies to our continued use of your data;
c) where you object to the processing (see below) and the organisation has no overriding legitimate interest to continue the processing;
d) where we have unlawfully processed your data;
e) where we are required by law to erase the data.

If you wish to make a request for data deletion, you should complete the Data Erasure form.

We will consider each request individually, however, you must be aware that processing may continue under one of the permissible reasons. Where this happens, you will be informed of the continued use of your data and the reason for this.

Third parties to whom the data was disclosed will be informed of the erasure where possible unless to do so will cause a disproportionate effect on us.

F) THE RIGHT OF 'RESTRICTION'

You have the right to restrict the processing of your data in certain circumstances.

We will be required to restrict the processing of your personal data in the following circumstances:

a) where you tell us that the data we hold on you is not accurate. Where this is the case, we will stop processing the data until we have taken steps to ensure that the data is accurate;
b) where the data is processed for the performance of a public interest task or because of our legitimate interests and you have objected to the processing of data. In these circumstances, the processing may be restricted whilst we consider whether our legitimate interests mean it is appropriate to continue to process it;
c) when the data has been processed unlawfully;
d) where we no longer need to process the data but you need the data in relation to a legal claim.

If you wish to make a request for data restriction, you should complete the Data Restriction form.

Where data processing is restricted, we will continue to hold the data but will not process it unless you consent to the processing or processing is required in relation to a legal claim.

Where the data to be restricted has been shared with third parties, we will inform those third parties of the restriction where possible unless to do so will cause a disproportionate effect on us.

You will be informed before any restriction is lifted.

G) THE RIGHT TO DATA 'PORTABILITY'

You have the right to obtain the data that we process on you and transfer it to another party. Where our technology permits, we will transfer the data directly to the other party.

Data which may be transferred is data which:

a) you have provided to us; and
b) is processed because you have provided your consent or because it is needed to perform the employment contract between us; and
c) is processed by automated means.

If you wish to exercise this right, please speak to your manager.

We will respond to a portability request without undue delay, and within one month at the latest unless the request is complex or we receive a number of requests in which case we may write to you to inform you that we require an extension and reasons for this. The maximum extension period is two months.

We will not charge you for access to your data for this purpose.

You will be informed if we decide not to take any action as a result of the request, for example, because the data you wish to transfer does not meet the above criteria. In these circumstances, you are able to complain to the Information Commissioner and have access to a judicial remedy.

The right to data portability relates only to data defined as above. You should be aware that this differs from the data which is accessible via a Subject Access Request.

H) THE RIGHT TO 'OBJECT'

You have a right to require us to stop processing your data; this is known as data objection.

You may object to processing where it is carried out:

a) in relation to the organisation's legitimate interests;
b) for the performance of a task in the public interest;
c) in the exercise of official authority; or
d) for profiling purposes.

If you wish to object, you should do so by completing the Data Objection Form.

In some circumstances we will continue to process the data you have objected to. This may occur when:

a) we can demonstrate compelling legitimate reasons for the processing which are believed to be more important than your rights; or
b) the processing is required in relation to legal claims made by, or against, us.

If the response to your request is that we will take no action, you will be informed of the reasons.

I) RIGHT NOT TO HAVE AUTOMATED DECISIONS MADE ABOUT YOU

You have the right not to have decisions made about you solely on the basis of automated decision making processes where there is no human intervention, where such decisions will have a significant effect on you.

We currently do not make decisions about you using automatic system involving no human intervention.

However, we may carry out automated decision making with no human intervention in the following circumstances:

a) when it is needed for entering into or the carrying out of a contract with you;
b) when the process is permitted by law;
c) when you have given explicit consent.

In circumstances where we use special category data, for example, data about your health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership the organisation will ensure that one of the following applies to the processing:

a) you have given your explicit consent to the processing; or
b) the processing is necessary for reasons of substantial public interest.

SUBJECT ACCESS REQUEST POLICY

A) AIM

You have a right, under the General Data Protection Regulation, to access the personal data we hold on you. To do so, you should made a subject access request, and this policy sets out how you should make a request, and our actions upon receiving the request.

B) DEFINITIONS

"Personal data" is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, including your name.

"Special categories of personal data" includes information relating to:

a) race
b) ethnic origin
c) politics
d) religion
e) trade union membership
f) genetics
g) biometrics (where used for ID purposes)
h) health
i) sex life or
j) sexual orientation.

C) MAKING A REQUEST

Although subject access requests may be made verbally, we would advise that a request may be dealt with more efficiently and effectively if it is made in writing. If you wish to make a request, please use the Subject Access Request form.

Requests that are made directly by you should be accompanied by evidence of your identity. If this is not provided, we may contact you to ask that such evidence be forwarded before we comply with the request.

Requests made in relation to your data from a third party should be accompanied by evidence that the third party is able to act on your behalf. If this is not provided, we may contact the third party to ask that such evidence be forwarded before we comply with the request.

D) TIMESCALES

Usually, we will comply with your request without delay and at the latest within one month. Where requests are complex or numerous, we may contact you to inform you that an extension of time is required. The maximum extension period is two months.

E) FEE

We will normally comply with your request at no cost. However, if the request is manifestly unfounded or excessive, or if it is repetitive, we may contact you requesting a fee. This fee must be paid in order for us to comply with the request. The fee will be determined at the relevant time and will be set at a level which is reasonable in the circumstances.

In addition, we may also charge a reasonable fee if you request further copies of the same information.

PRIVACY NOTICE FOR EMPLOYEES/WORKERS

In accordance with the General Data Protection Regulation (GDPR), we have implemented this privacy notice to inform you, our employees, of the types of data we process about you. We also include within this notice the reasons for processing your data, the lawful basis that permits us to process it, how long we keep your data for and your rights regarding your data.

This notice applies to current and former employees and workers.

A) DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a) processing is fair, lawful and transparent
b) data is collected for specific, explicit, and legitimate purposes

c) data collected is adequate, relevant and limited to what is necessary for the purposes of processing
d) data is kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
e) data is not kept for longer than is necessary for its given purpose
f) data is processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
g) we comply with the relevant GDPR procedures for international transferring of personal data

B) TYPES OF DATA HELD

We keep several categories of personal data on our employees in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the data within our computer systems, for example, our holiday booking system.

Specifically, we hold the following types of data, as appropriate to your status:

a) personal details such as name, address, phone numbers
b) name and contact details of your next of kin
c) your photograph
d) your gender, marital status, information of any disability you have or other medical information
e) right to work documentation
f) information on your race and religion for equality monitoring purposes
g) information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter
h) references from former employers
i) details on your education and employment history etc
j) National Insurance numbers
k) bank account details
l) tax codes
m) driving licence
n) criminal convictions
o) information relating to your employment with us, including:

i) job title and job descriptions
ii) your salary
iii) your wider terms and conditions of employment
iv) details of formal and informal proceedings involving you such as letters of concern, disciplinary and grievance proceedings, your annual leave records, appraisal and performance information
v) internal and external training modules undertaken
vi) information on time off from work including sickness absence, family related leave etc

p) CCTV footage
q) building access card records
r) IT equipment use including telephones and internet access.

C) COLLECTING YOUR DATA

You provide several pieces of data to us directly during the recruitment period and subsequently upon the start of your employment.

In some cases, we will collect data about you from third parties, such as employment agencies, former employers when gathering references or credit reference agencies.

Personal data is kept in files or within the Company's HR and IT systems.

D) LAWFUL BASIS FOR PROCESSING

The law on data protection allows us to process your data for certain reasons only. In the main, we process your data in order to comply with a legal requirement or in order to effectively manage the employment contract we have with you, including ensuring you are paid correctly.

The information below categorises the types of data processing, appropriate to your status, we undertake and the lawful basis we rely on.

Activity requiring your data	Lawful basis
Carry out the employment contract that we have entered into with you e.g. using your name, contact details, education history, information on any disciplinary, grievance procedures involving you	Performance of the contract
Ensuring you are paid	Performance of the contract
Ensuring tax and National Insurance is paid	Legal obligation
Carrying out checks in relation to your right to work in the UK	Legal obligation
Making reasonable adjustments for disabled employees	Legal obligation
Making recruitment decisions in relation to both initial and subsequent employment e.g. promotion	Our legitimate interests
Making decisions about salary and other benefits	Our legitimate interests
Ensuring efficient administration of contractual benefits to you	Our legitimate interests
Effectively monitoring both your conduct, including timekeeping and attendance, and your performance and to undertake procedures where necessary	Our legitimate interests

Maintaining comprehensive up to date personnel records about you to ensure, amongst other things, effective correspondence can be achieved and appropriate contact points in the event of an emergency are maintained	Our legitimate interests
Implementing grievance procedures	Our legitimate interests
Assessing training needs	Our legitimate interests
Implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken including the making of reasonable adjustments	Our legitimate interests
Gaining expert medical opinion when making decisions about your fitness for work	Our legitimate interests
Managing statutory leave and pay systems such as maternity leave and pay etc.	Our legitimate interests
Business planning and restructuring exercises	Our legitimate interests
Dealing with legal claims made against us	Our legitimate interests
Preventing fraud	Our legitimate interests
Ensuring our administrative and IT systems are secure and robust against unauthorised access	Our legitimate interests
Providing employment references to prospective employers, when our name has been put forward by the employee/ex-employee, to assist with their effective recruitment decisions	Legitimate interest of the prospective employer

E) SPECIAL CATEGORIES OF DATA

Special categories of data are data relating to your:

a) health
b) sex life
c) sexual orientation
d) race
e) ethnic origin
f) political opinion
g) religion
h) trade union membership
i) genetic and biometric data.

We carry out processing activities using special category data:

a) for the purposes of equal opportunities monitoring
b) in our sickness absence management procedures
c) to determine reasonable adjustments

Most commonly, we will process special categories of data when the following applies:

a) you have given explicit consent to the processing
b) we must process the data in order to carry out our legal obligations
c) we must process data for reasons of substantial public interest
d) you have already made the data public.

F) FAILURE TO PROVIDE DATA

Your failure to provide us with data may mean that we are unable to fulfil our requirements for entering into a contract of employment with you. This could include being unable to offer you employment, or administer contractual benefits.

G) CRIMINAL CONVICTION DATA

We will only collect criminal conviction data where it is appropriate given the nature of your role and where the law permits us. This data will usually be collected at the recruitment stage, however, may also be collected during your employment. We use criminal conviction data to determine your suitability, or your continued suitability for the role. We rely on the lawful basis of our legitimate interests to process this data.

H) WHO WE SHARE YOUR DATA WITH

Employees within our company who have responsibility for recruitment, administration of payment and contractual benefits and the carrying out performance related procedures will have access to your data which is relevant to their function. All employees with such responsibility have been trained in ensuring data is processed in line with GDPR.

Data is shared with third parties for the following reasons: the administration of payroll – DBS checks

We may also share your data with third parties as part of a Company sale or restructure, or for other reasons to comply with a legal obligation upon us. We have a data processing agreement in place with such third parties to ensure data is not compromised. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

We may share your data with bodies outside of the European Economic Area. These countries are worldwide and the reason for sharing with these countries is to comply with any legal requirement – to assist with any law enforcement organisation at our discretion. We have put the following measures in place to ensure that your data is transferred securely and that the bodies who receive the data that we have transferred process it in a way required by EU and UK data protection laws:

Only via secure encrypted email, or passcode protected storage device

I) PROTECTING YOUR DATA

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such.

J) RETENTION PERIODS

We only keep your data for as long as we need it for, which will be at least for the duration of your employment with us though in some cases we will keep your data for a period after your employment has ended. Some data retention periods are set by the law. Retention periods can vary depending on why we need your data, as set out below:

Reference to you in any document that was created whilst you were employed with us that we require to maintain for either operational or legal purposes.

K) AUTOMATED DECISION MAKING

Automated decision making means making decision about you using no human involvement e.g. using computerised filtering equipment. No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

L) EMPLOYEE RIGHTS

You have the following rights in relation to the personal data we hold on you:

a) the right to be informed about the data we hold on you and what we do with it;
b) the right of access to the data we hold on you. More information on this can be found in our separate policy on Subject Access Requests;
c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
d) the right to have data deleted in certain circumstances. This is also known as 'erasure';
e) the right to restrict the processing of the data;
f) the right to transfer the data we hold on you to another party. This is also known as 'portability';
g) the right to object to the inclusion of any information;
h) the right to regulate any automated decision-making and profiling of personal data.

More information can be found on each of these rights in our separate policy on employee rights under GDPR.

M) CONSENT

Where you have provided consent to our use of your data, you also have the right to withdraw that consent at any time. This means that we will stop processing your data.

N) MAKING A COMPLAINT

If you think your data rights have been breached, you are able to raise a complaint with the Information Commissioner (ICO). You can contact the ICO at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by telephone on 0303 123 1113 (local rate) or 01625 545 745.

O) DATA PROTECTION COMPLIANCE

Our appointed compliance officer in respect of our data protection activities is:

Chief Executive whom can be contacted via the Disability Action Haringey office.

DATA BREACH NOTIFICATION POLICY

A) AIM

We are aware of the obligations placed on us by the General Data Protection Regulation (GDPR) in relation to processing data lawfully and to ensure it is kept securely.

One such obligation is to report a breach of personal data in certain circumstances and this policy sets out our position on reporting data breaches.

B) PERSONAL DATA BREACH

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed.

The following are examples of data breaches:

a) access by an unauthorised third party;
b) deliberate or accidental action (or inaction) by a data controller or data processor;
c) sending personal data to an incorrect recipient;
d) computing devices containing personal data being lost or stolen;
e) alteration of personal data without permission;
f) loss of availability of personal data.

C) BREACH DETECTION MEASURES

We have implemented the following measures to assist us in detecting a personal data breach: Software and malware protection – password protection on data – lockable cabinets

D) INVESTIGATION INTO SUSPECTED BREACH

In the event that we become aware of a breach, or a potential breach, an investigation will be carried out. This investigation will be carried out by Chief executive in conjunction with our IT service provider, the Chair will be notified whom in conjunction with the Chief Executive will make a decision over whether the breach is required to be notified to the Information Commissioner. A decision will also be made over whether the breach is such that the individual(s) must also be notified.

E) WHEN A BREACH WILL BE NOTIFIED TO THE INFORMATION COMMISSIONER

In accordance with the GDPR, we will undertake to notify the Information Commissioner of a breach which is likely to pose a risk to people's rights and freedoms. A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.

Notification to the Information Commissioner will be done without undue delay and at the latest within 72 hours of discovery. If we are unable to report in full within this timescale, we will make an initial report to the Information Commissioner, and then provide a full report in more than one instalment if so required.

The following information will be provided when a breach is notified:

a) a description of the nature of the personal data breach including, where possible:

   i) the categories and approximate number of individuals concerned; and
   ii) the categories and approximate number of personal data records concerned

b) the name and contact details of the appointed compliance officer where more information can be obtained;
c) a description of the likely consequences of the personal data breach; and
d) a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

F) WHEN A BREACH WILL BE NOTIFIED TO THE INDIVIDUAL

In accordance with the GDPR, we will undertake to notify the individual whose data is the subject of a breach if there is a *high* risk to people's rights and freedoms. A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.

This notification will be made without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.

The following information will be provided when a breach is notified to the affected individuals:

a) a description of the nature of the breach
b) the name and contact details of the appointed compliance officer where more information can be obtained
c) a description of the likely consequences of the personal data breach and
d) a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

G) RECORD OF BREACHES

The Company records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under GDPR. It records the facts relating to the breach, its effects and the remedial action taken.

Date of next Review: March 2027