One Place East

Where disability matters

Data Protection Policy

February 2024
Next review date February 2027

Introduction

This Policy sets out the obligations of One Place East, an Organisation registered in England under number 3115971, whose registered office is at Ilford Chambers, 11 Chapel Road, Ilford, IG1 2DR (“the Organisation”) regarding data protection and the rights of service users, staff, volunteers, funders, customers and suppliers (“data subjects”) in respect of their personal data under the Data Protection Act 2018 (The Act).

The Act defines “personal data” as any information held in either electronic or paper form relating to an identified or identifiable natural person (a “data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, address, date of birth, National Insurance Number, passport, bank details, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The Act also addresses “special category” personal data (also known as “sensitive” personal data). Such data includes, but is not necessarily limited to, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), the commission or alleged commission of offences or their physical or mental health, sex life, or sexual orientation.

This Policy sets the Organisation’s obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Organisation, its employees, agents, contractors, or other parties working on behalf of the Organisation.

The Organisation is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

The Data Protection Principles

This Policy aims to ensure compliance with the Act. The Act sets out the following principles with which any party handling personal data must comply. All personal data must be:

- Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

- 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.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 the data subject.
- 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.

The Rights of Data Subjects

The Act sets out the following rights applicable to data subjects (please refer to the specific section of the policy for further details):

- The right to be informed – Keeping Data Subjects Informed (see page 7).
- The right of access – Data Subject Access (see page 8).
- The right to rectification – Rectification of Personal Data (see page 9).
- The right to erasure (also known as the ‘right to be forgotten’) – Erasure of Personal Data (see page 9).
- The right to restrict processing – Restriction of Personal Data Processing (see page 10).

- The right to data portability – Data Portability (see page 10).
- The right to object – Objections to Personal Data Processing (see page 11).
- Rights with respect to automated decision-making and profiling – Automated Decision Making (see page 11).

Lawful, Fair, and Transparent Data Processing

The Act seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Act states that processing of personal data shall be lawful if at least one of the following applies:

- The data subject has given consent to the processing of their personal data for one or more specific purposes.
- The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them.
- The processing is necessary for compliance with a legal obligation to which the data controller is subject.
- The processing is necessary to protect the vital interests of the data subject or of another natural person.
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.
- The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

If the personal data in question is “special category data” (also known as “sensitive personal data”) (for example, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

- The data subject has given their explicit consent to the processing of such data for one or more specified purposes.

- The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law.
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects.
- The processing relates to personal data which is clearly made public by the data subject.
- The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity.
- The processing is necessary for substantial public interest reasons, on the basis of The Act which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.
- The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of the Act pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Schedule 2 of the Act.
- The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of the Act which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy).
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical

purposes in accordance with Schedule 2 of the Act which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Specified, Explicit, and Legitimate Purposes

The Organisation collects and processes the personal data set out in the table on page 11 of this Policy. This includes:

- Personal data collected directly from data subjects
- Personal data obtained from third parties.

The Organisation only collects, processes, and holds personal data for the specific purposes set out on page 11 of this Policy (or for other purposes expressly permitted by the Act).

Data subjects are kept informed at all times of the purpose or purposes for which the Organisation uses their personal data. Please refer to page 7 for more information on keeping data subjects informed.

Adequate, Relevant, and Limited Data Processing

The Organisation will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed).

Accuracy of Data and Keeping Data Up-to-Date

The Organisation shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out on page 9.

The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

Data Retention

The Organisation shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

For full details of the Organisation's approach to data retention, including retention periods for specific personal data types held by the Organisation, please refer to our Data Retention Policy.

Secure Processing

The Organisation shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided on pages 14 - 17 of this Policy.

Accountability and Record-Keeping

The Organisation's Data Protection Officer is Margaret Summers, margaret.summers@oneplaceeast.org, 020 8925 2435.

The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Organisation's other data protection-related policies, and with the Act and other applicable data protection legislation.

The Organisation shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- The name and details of the Organisation, its Data Protection Officer, and any applicable third-party data processors.
- The purposes for which the Organisation collects, holds, and processes personal data.
- Details of the categories of personal data collected, held, and processed by the Organisation, and the categories of data subject to which that personal data relates.
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards.
- Details of how long personal data will be retained by the Organisation (please refer to the Organisation's Data Retention Policy).
- Detailed descriptions of all technical and organisational measures taken by the Organisation to ensure the security of personal data.

Data Protection Impact Assessments

The Organisation shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data.

Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

- The type(s) of personal data that will be collected, held, and processed.
- The purpose(s) for which personal data is to be used.
- The Organisation's objectives.
- How personal data is to be used.
- The parties (internal and/or external) who are to be consulted.
- The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed.
- Risks posed to data subjects.
- Risks posed both within and to the Organisation.
- Proposed measures to minimise and handle identified risks.

Keeping Data Subjects Informed

The Organisation shall provide the following information to every data subject:

- Details of the Organisation including, but not limited to, the identity of its Data Protection Officer.
- The purpose(s) for which the personal data is being collected and will be processed (as detailed in the table on page 11 of this Policy) and the legal basis justifying that collection and processing.
- Where applicable, the legitimate interests upon which the Organisation is justifying its collection and processing of the personal data.
- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed.
- Where the personal data is to be transferred to one or more third parties, details of those parties.
- Where the personal data is to be transferred to a third party that is located in a third country, details of that transfer, including but not

limited to the safeguards in place (see page 16 of this Policy for further details).

- Details of data retention.
- Details of the data subject's rights under the Act.
- Details of the data subject's right to withdraw their consent to the Organisation's processing of their personal data at any time.
- Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the Act).
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it.
- Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection.

Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

- if the personal data is used to communicate with the data subject, when the first communication is made; or
- if the personal data is to be transferred to another party, before that transfer is made; or
- as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

Data Subject Access

- Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Organisation holds about them, what it is doing with that personal data, and why.
- Data subjects wishing to make a SAR may do so in writing, using the Organisation's Subject Access Request Form, or other written communication. SARs should be addressed to the Organisation's Data Protection Officer - Margaret Summers,

margaret.summers@oneplaceeast.org, 020 8925 2435.

- Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.
- All SARs received shall be handled by the Organisation's Data Protection Officer.
- The Organisation does not charge a fee for the handling of normal SARs. The Organisation reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

Rectification of Personal Data

Data subjects have the right to require the Organisation to rectify any of their personal data that is inaccurate or incomplete.

The Organisation shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Organisation of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

Erasure of Personal Data

Data subjects have the right to request that the Organisation erases the personal data it holds about them in the following circumstances:

- It is no longer necessary for the Organisation to hold that personal data with respect to the purpose(s) for which it was originally collected or processed.
- The data subject wishes to withdraw their consent to the Organisation holding and processing their personal data.
- The data subject objects to the Organisation holding and processing their personal data (and there is no overriding legitimate interest to allow the Organisation to continue doing so) (see page 13 of this Policy for further details concerning the right to object).

- The personal data has been processed unlawfully.
- The personal data needs to be erased in order for the Organisation to comply with a particular legal obligation.

Unless the Organisation has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

Restriction of Personal Data Processing

Data subjects may request that the Organisation ceases processing the personal data it holds about them. If a data subject makes such a request, the Organisation shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

Data Portability

The Organisation does not process personal data using automated means.

To facilitate the right of data portability, the Organisation shall make available all applicable personal data to data subjects in the following format[s]:

- Encrypted data memory stick
- Hard copy
- Password protected email.

All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such

additional time is required, the data subject shall be informed.

Objections to Personal Data Processing

Data subjects have the right to object to the Organisation processing their personal data based on legitimate interests, direct marketing (including profiling).

Where a data subject objects to the Organisation processing their personal data based on its legitimate interests, the Organisation shall cease such processing immediately, unless it can be demonstrated that the Organisation's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

Where a data subject objects to the Organisation processing their personal data for direct marketing purposes, the Organisation shall cease such processing immediately.

Automated Decision-Making

The Organisation does not use automated decision-making processes.

Profiling

The Organisation does not use personal data for profiling purposes.

Personal Data Collected, Held, and Processed

The following personal data is collected, held, and processed by the Organisation (for details of data retention, please refer to the Organisation's Data Retention Policy):

Type of Data	Purpose of Data
Name	To enable contact with the data subject
Address	To enable contact with the data subject
Telephone number	To enable contact with the data subject
Email address	To enable contact with the data subject
Date of birth	Monitoring requirements for funders

Type of Data	Purpose of Data
Religion	Monitoring requirements for funders
Ethnic origin	Monitoring requirements for funders
Sexuality	Monitoring requirements for funders
Gender	Monitoring requirements for funders
Disability	Monitoring requirements for funders
NI number	Employment/payroll information
Salary	Employment/payroll information
Union membership	Employment/payroll information
Emergency contact	Employment/payroll information
Criminal record	Employment/payroll information

Data Security - Transferring Personal Data and Communications

The Organisation shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

- All emails containing personal data must be encrypted.
- All emails containing personal data must be marked “confidential”.
- Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable.
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.
- All personal data which needs to be physically taken from the office in hardcopy form will be kept in a secure manner ie locked briefcase.
- All personal data which needs to be physically taken from the office using removable electronic media shall be transferred via encrypted usb flash drive or password protected mobile device.

Data Security - Storage

The Organisation shall ensure that the following measures are taken with respect to the storage of personal data:

- All electronic copies of personal data should be stored securely using passwords and data encryption.
- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar.
- All personal data stored electronically should be backed up daily with backups stored onsite and offsite. All backups should be encrypted.
- Personal data should only be stored on a mobile device (including, but not limited to, laptops, tablets, and smartphones) belonging to the Organisation and in accordance with the requirements of the role
- No personal data should be transferred to any device personally belonging to an employee without prior written approval from the Organisation's Data Protection Officer.

Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Organisation's Data Retention Policy.

Data Security - Use of Personal Data

The Organisation shall ensure that the following measures are taken with respect to the use of personal data:

- No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Organisation requires access to any personal data that they do not already have access to, such access should be formally requested from Margaret Summers, margaret.summers@oneplaceeast.org, 020 8925 2435.
- No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on

behalf of the Organisation or not, without the authorisation of Margaret Summers.

- Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.
- Where personal data held by the Organisation is used for marketing purposes, it shall be the responsibility of the Chief Officer and or Project Manager to ensure that the appropriate consent is obtained and that no data subjects have opted out.

Data Security - IT Security

The Organisation shall ensure that the following measures are taken with respect to IT and information security:

- All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols as detailed in the IT Security Policy.
- Under no circumstances should any passwords be shared between any employees, agents, contractors, or other parties working on behalf of the Organisation. If a password is forgotten, it must be reset using the applicable method.
- All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Organisation's IT Support Provider shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so; and
- No software may be installed on any Organisation-owned computer or device without the prior approval of the IT Support Provider.
- More detailed information regarding IT Security can be found in the Organisation's IT Security Policy.

Organisational Measures

The Organisation shall ensure that the following measures are taken with

respect to the collection, holding, and processing of personal data:

- All employees, agents, contractors, or other parties working on behalf of the Organisation shall be made fully aware of both their individual responsibilities and the Organisation's responsibilities under the Act and under this Policy, and shall be provided with a copy of this Policy.
- Only employees, agents, sub-contractors, or other parties working on behalf of the Organisation that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Organisation.
- All employees, agents, contractors, or other parties working on behalf of the Organisation handling personal data will be appropriately trained to do so.
- All employees, agents, contractors, or other parties working on behalf of the Organisation handling personal data will be appropriately supervised.
- All employees, agents, contractors, or other parties working on behalf of the Organisation handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise.
- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed.
- All personal data held by the Organisation shall be reviewed periodically, as set out in the Organisation's Data Retention Policy.
- The performance of those employees, agents, contractors, or other parties working on behalf of the Organisation handling personal data shall be regularly evaluated and reviewed.
- All employees, agents, contractors, or other parties working on behalf of the Organisation handling personal data will be bound to do so in accordance with the principles of the Act and this Policy by contract.
- All agents, contractors, or other parties working on behalf of the Organisation handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Organisation arising out of this Policy and the Act.
- Where any agent, contractor or other party working on behalf of the Organisation handling personal data fails in their obligations under

this Policy that party shall indemnify and hold harmless the Organisation against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

Transferring Personal Data to a Third Country

The Organisation may from time to time transfer ('transfer' includes making available remotely) personal data to third countries.

The transfer of personal data to a third country shall take place only if one or more of the following applies:

- The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data.
- The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Act); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.
- The transfer is made with the informed consent of the relevant data subject(s).
- The transfer is necessary for the performance of a contract between the data subject and the Organisation (or for pre-contractual steps taken at the request of the data subject).
- The transfer is necessary for important public interest reasons.
- The transfer is necessary for the conduct of legal claims.
- The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent.
- The transfer is made from a register that, under UK law, is intended to provide information to the public and which is open for access by

the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

Data Breach Notification

All personal data breaches must be reported immediately to the Organisation's Data Protection Officer.

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described above) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned.
- The categories and approximate number of personal data records concerned.
- The name and contact details of the Organisation's data protection officer (or other contact point where more information can be obtained).
- The likely consequences of the breach.
- Details of the measures taken, or proposed to be taken, by the Organisation to address the breach including, where appropriate, measures to mitigate its possible adverse effects.