HR Procedure HRP: 18a **General Data Protection**

Document Description

This document outlines our legal requirements under the General Data Protection Regulations and the processes for how Ceiba Community Support meets them. Implementation is immediate, and this Policy shall stay in force until any alterations are formally agreed. The Policy will be reviewed every two years by the Board of Directors and the Data Protection Officer,sooner if legislation, best practice or other circumstances indicate this is necessary. All aspects of this Policy shall be open to review at any time. If you have any comments or suggestions on the content of this policy please contact, our Registered Manager - Weronika Pawlowicz at weronika@ceibacommunitysupport.co.uk and/or our Administrator (Data Protection Officer) - Ilona Kaminska at office@ceibacommunitysupport.co.uk.

The UK GDPR is the UK General Data Protection Regulation. It is a UK law which came into effect on 01 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK.
It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679) which applied in the UK before that date, with some changes to make it work more effectively in a UK context.

The Data Protection Act (DPA) 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018. It was amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU.

All Ceiba Community Support staff are required to follow the UK General Data Protection Regulation and The Data Protection Act 2018 at all times.

Definitions

Processing of information – how information is held and managed.
Information Commissioner - formerly known as the Data Protection Commissioner.
Notification – formerly known as Registration.
Data Subject – used to denote an individual about whom data is held.
Data Controller – used to denote the entity with overall responsibility for data collection and management. Ceiba Community Support is the Data Controller for the purposes of the Act.
Data Processor – an individual handling or processing data
Personal data – any information which enables a person to be identified.
Sensitive personal data - includes personal data about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical or mental health condition, sexual orientation or sexual life. It can also include data about criminal offences or convictions. Sensitive personal data can only be processed under strict conditions, including with the consent of the individual.
Special categories of personal data – information under the Regulations which requires the individual's explicit consent for it to be held by the Company.

Data Protection Principles

As data controller, Ceiba Community Support is required to comply with the principles of good information handling.

These principles require the Data Controller to:

1. Process personal data fairly, lawfully and in a transparent manner.
2. Obtain personal data only for one or more specified and lawful purposes and to ensure that such data is not processed in a manner that is incompatible with the purpose or purposes for which it was obtained.
3. Ensure that personal data is adequate, relevant, and not excessive for the purpose or purposes for which it is held.
4. Ensure that personal data is accurate and, where necessary, kept up-to-date.
5. Ensure that personal data is not kept for any longer than is necessary for the purpose for which it was obtained.
6. Ensure that personal data is kept secure.
7. Ensure that personal data is not transferred to a country outside the European Economic Area unless the country to which it is sent ensures an adequate level of protection for the rights (in relation to the information) of the individuals to whom the personal data relates.

1. INTRODUCTION

1.1 To allow Ceiba Community Support to carry out its duties, rights and obligations as an employer, employees may be required to give certain personal information. We will process and control such information principally for personnel, administrative and payroll purposes.

1.2 The term 'processing' may include us obtaining, recording or holding information or data or carrying out any set operation or operations on the information or data. This may include organizing, altering, retrieving, consulting, using, disclosing, or destroying the information or data. We will adopt appropriate technical and organizational measures to prevent the unauthorized or unlawful processing or disclosure of data.

1.3 It may be necessary to transfer data relating to employees outside of the UK in order that we may properly carry out our duties, rights and obligations, in the following circumstances:

- Employees accompanying Service Users on holiday abroad.

1.4 Employees are requested to sign a Consent Form which allows us to process data relating to them, which may include sensitive data.

2. OBTAINING CONSENT

2.1. Consent may be obtained in several ways depending on the nature of the interview, and consent must be recorded on or maintained with the case records:

- face-to-face; pro-forma should be used
- written; as above
- telephone; verbal consent should be sought and noted on the case record
- email; the initial response should seek consent

2.2 Individuals have a right to withdraw consent at any time. If this affects the provision of a service by Ceiba Community Support, then this should be discussed with the client at the earliest opportunity

3. ENSURING THE SECURITY OF PERSONAL INFORMATION

3.1 It is an offence to disclose personal information 'knowingly and recklessly' to third parties

3.2 It is a condition of receiving a service that all service users for whom we hold personal details sign a consent form allowing us to hold such information.

3.3 Service users may also consent for us to share personal or special categories of personal information with other helping agencies on a need to know basis.

3.4. A client's individual consent to share information should always be checked before disclosing personal information to another agency.

3.5 Where such consent does not exist information may only be disclosed if it is in connection with criminal proceedings or to prevent substantial risk to the individual concerned. In either case permission of the Registered Manager or Operations Manager should first be sought.

3.5 Personal information should only be communicated within Ceiba`s staff on a strict need to know basis. Care should be taken that conversations containing personal or special categories of personal information may not be overheard by people who should not have access to such information.

4. DATA SECURITY

4.1. We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

4.2 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

a. **Confidentiality** means that only people who are authorised to use the data can access it.
b. **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
c. **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the Company`s central computer system instead of individual PCs.

4.3 Security procedures include:

a. **Entry controls.** Any stranger seen in the office should be reported.
b. **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
c. **Clean Desk Policy** should be adhered to by staff.
d. **Data minimisation.**
e. **Pseudonymisation and encryption of data.**
f. **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
g. **Equipment.** Staff must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
   The software should be kept up-to-date.
   Unexpected or suspicious email attachments should never be opened. Malware and viruses can be easily downloaded through malicious attachments or links.
h. **Data Backup Policy** should be adhered to by Ceiba staff.

5. SUBJECT ACCESS REQUESTS

5.1 Individuals must make a formal request for information we hold about them.

5.2. When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

a. We will check the caller's identity to make sure that information is only given to a person who is entitled to it.
b. We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

5.3. Where a request is made electronically, data will be provided electronically where possible.

6. RETENTION OF RECORDS

6.1 Paper records should be retained for the following periods at the end of which they should be shredded:

- Client records – 6 years after ceasing to be a client.
- Staff records – 6 years after ceasing to be a member of staff.
- Unsuccessful staff application forms – 6 months after vacancy closing date.
- Volunteer records – 6 years after ceasing to be a volunteer.
- Timesheets and other financial documents – 6 years from the end of the tax year to which they relate.
- Employer's liability insurance – permanent retention applies.
- Accident books, accident records/reports -3 years from the last entry
- Other documentation, eg clients care plan sent to a worker as briefing for a visit, should be destroyed as soon as it is no longer needed for the task in hand.

7. DATA PROTECTION BREACH

7.1 If you discover, or suspect, a data protection breaches you should report this to your line manager who will review our systems, in conjunction with the Registration Manager and the Data Protection Officer, to prevent a reoccurrence.

The Registered Manager and the Data Protection Officer should be informed of the breach. An appropriate action should be taken to determine whether it needs to be reported to the Information Commissioner. There is a time limit for reporting breaches to ICO so the Registered Manager should be informed without delay.

7.2 Any deliberate or reckless breach of this Data Protection Policy by an employee may result in disciplinary action which may result in dismissal.