2.9 Data Protection Policy

2.9.1 Introduction

EBP South needs to collect and use certain types of information about the Individuals or Service Users who come into contact with EBP South in order to carry on our work. This personal information must be collected and dealt with appropriately whether **it** is collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under the Data Protection Act 2018.

2.9.2 Data Controller

EBP South is the Data Controller under the Act, which means that it determines what purposes personal information held, will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

2.9.3. Disclosure

EBP South in specific circumstances may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Individual/Service User will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows EBP South to disclose data (including sensitive data) without the data subject's consent.

These are:

- Carrying out a legal duty or as authorised by the Secretary of State.
- Protecting vital interests of an Individual/Service User or other person (Safeguarding).
- The Individual/Service User has already made the information public.
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights.
- Monitoring for equal opportunities purposes – i.e. race, disability or religion.
- Providing a confidential service where the Individual/Service User's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Individuals/Service Users to provide consent signatures.

EBP South regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

EBP South intends to ensure that personal information is treated lawfully and correctly.

To this end, EBP South will adhere to the Principles of Data Protection, as detailed in the Data Protection Act 2018.

Specifically, the Principles require that personal information:

- Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met.
- Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes.
- Shall be adequate, relevant and not excessive in relation to those purpose(s).
- Shall be accurate and, where necessary, kept up to date.
- Shall not be kept for longer than is necessary.
- Shall be processed in accordance with the rights of data subjects under the Act.
- Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information.
- Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Individuals/Service Users in relation to the processing of personal information.

EBP South will, through appropriate management and strict application of criteria and controls**:**

- Observe fully conditions regarding the fair collection and use of information.
- Meet its legal obligations to specify the purposes for which information is used.
- Collect and process appropriate information, and only to the extent that it is needed to fulfill its operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:
    - The right to be informed that processing is being undertaken.
    - The right of access to one's personal information.
    - The right to prevent processing in certain circumstances.
    - The right to correct, rectify, block or erase information which is regarded as wrong information.

- Take appropriate technical and organisational security measures to safeguard personal information.

- Ensure that personal information is not transferred abroad without suitable safeguards.

- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.

- Set out clear procedures for responding to requests for information.

2.9.4 Data collection

Informed consent is when an individual/service user clearly understands:

- Why their information is needed.

- Who it will be shared with.

- The possible consequences of them agreeing or refusing the proposed use of the data.

- Gives their consent

EBP South will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, EBP South will ensure that the Individual/Service User:

- Clearly understands why the information is needed.

- Understands what it will be used for and what the consequences are should the Individual/Service User decide not to give consent to processing.

- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed.

- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress.

- Has received sufficient information on why their data is needed and how it will be used.

2.9.5 Data Storage

Information and records relating to service users will be stored securely and will only be accessible to authorised employees and volunteers.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is EBP South's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

2.9.6 Data access and accuracy

All Individuals/Service Users have the right to access the information EBP South holds about them. EBP South will also take reasonable steps to ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition**,** EBP South will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection.
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice.
- Everyone processing personal information is appropriately trained to do so.
- Everyone processing personal information is appropriately supervised
- Anybody wanting to make enquiries about handling personal information knows what to do
- It deals promptly and courteously with any enquiries about handling personal information
- It describes clearly how it handles personal information
- It will regularly review and audit the ways it hold, manage and use personal information
- It regularly assesses and evaluates its methods and performance in relation to handling personal information
- All employees are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 2018.

In case of any queries or questions in relation to this policy please contact EBP South's Data Protection Officer: Sammy Ward

Date of last review: March 2023
Date of next review: Currently under review

Glossary of Terms

Data Controller – The person who (either alone or with others) decides what personal information Basingstoke Consortium and EBP South will hold and how it will be held or used.

Data Protection Act 2018 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person(s) responsible for ensuring that Basingstoke Consortium and EBP South follows its data protection policy and complies with the Data Protection Act 2018.

Individual/Service User – The person whose personal information is being held or processed by Basingstoke Consortium and EBP South for example: a client, an employee, or supporter.

Explicit consent – is a freely given, specific and informed agreement by an Individual/Service User in the processing of personal information about her/him. Explicit consent is needed for processing sensitive data.

Notification – Notifying the Information Commissioner about the data processing activities of Basingstoke Consortium and EBP South, as certain activities may be exempt from notification.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 2018.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees within Basingstoke Consortium and EBP South.

Sensitive data – refers to data about:

- Racial or ethnic origin
- Political affiliations
- Religion or similar beliefs
- Trade union membership
- Physical or mental health
- Sexuality
- Criminal record or proceedings

Confidential Information - Privileged communication shared with only a few people for furthering certain purposes, such as with an attorney for a legal matter, or with a doctor for treatment of a disease. Receiver of confidential information is generally prohibited from using it to take advantage of the giver.

Data Protection Procedures

Clear Desk, Clear Screen Procedure

At the end of each day, or when desks/offices are unoccupied, any 'confidential' information must be locked away in either pedestals or filing cabinets, as appropriate.

All waste paper, which has any personal or confidential information or data on, must be shredded. Under no circumstances should this type of waste paper be thrown away with normal rubbish in the waste paper bins.

Whenever you leave your desk and your PC is switched on, it is essential that you **ALWAYS** 'lock' your screen by pressing 'Ctrl, Alt, Delete' and then enter, to confirm that you wish to 'lock' your workstation.

Locking your screen not only prevents someone else from using your PC, which is logged on in your name, but it also prevents someone from reading confidential information left open on your screen, .

If working on sensitive information, and you have a visitor to your desk, lock you screen to prevent the contents being read.

Data Transfers

Data transfers should, where possible, only take place via secure on-line channels where the data is encrypted rather than copying to media. Manual data transfers using removable physical media (e.g. memory sticks, CDs, tape, etc.) should end where possible. In the meantime, where data is copied to removable media such data must be encrypted using the strongest possible encryption method available. Strong passwords/passphrases must be used to encrypt/decrypt the data.

Laptops and Other Mobile Storage Devices (incl. Mobile Phones, USB memory sticks, External Hard Drives, etc.)

Mobile storage devices are useful tools to meet the business needs of employees however, they are highly susceptible to loss or theft. To protect the content held on these devices, the following recommendations should be followed:

1. All portable devices should be password-protected to prevent unauthorised use of the device and unauthorised access to information held on the device. In the case of mobile phones, a PIN should be used.

2. Passwords used on these devices should be of sufficient strength to deter password cracking or guessing attacks. A password should include numbers, symbols, upper and lowercase letters. Password length should ideally be around 12 to 14 characters but at the very minimum 8 characters. Passwords based on repetition, dictionary words, letter or number sequences, usernames, or biographical information like names or dates must be avoided. You must ensure that passwords are regularly changed.

3. Personal, private, sensitive or confidential data should not be stored on portable devices. In cases where this is unavoidable, all devices containing this type of data must be

encrypted. With regard to laptops, full disk encryption must be employed regardless of the type of data stored.

4. When portable computing devices are being used in public places, care must be taken to avoid unwitting disclosure of information, e.g. through overlooking or overhearing by unauthorised persons.

6. Anti-virus/Anti-spyware/Personal Firewall software must be installed and kept up to date on portable devices. These devices should be subjected to regular virus checks using this software.

7. Laptops must be physically secured if left in the office overnight. When out of the office, the device should be kept secure at all times.

8. Portable devices should never be left in an unattended vehicle.

9. Portable storage media should only be used for personal or sensitive data transfer where there is a business requirement to do so and must be encrypted.

10. Remote access to EBP South's filing systems must be approved by a Senior Manager and must be fully password protected. Access will be granted based on business need.

Hosting on External Sites (inc. Google Docs, Dropbox)

Personal Information, Confidential Information and Sensitive Data is not to be stored on external sites.