Data Protection Policy

Date submitted to Management Team: **March 2014**

Policy to take effect from: **March 2014**

To be reviewed: **February 2017**

Version No. **4.0**

Introduction
EPIC Ltd holds personal and confidential information about its employees, board members, employment applicants, tenants, housing applicants and suppliers. All individuals have a right to privacy and EPIC is bound by the Data Protection Act 1998.

The policy covers all records and information held by EPIC concerning confidentiality in respect of information held in relation to employees, board members, employment applicants, tenants, housing applicants and suppliers.

Aims of the Policy
This policy aims to protect and promote the rights of individuals and EPIC. It identifies information that is to be treated as confidential and the procedures for collecting, storing, handling and disclosing such information.

Policy Statement

Data Protection
EPIC holds confidential information relating to all employees. Most detailed information may be held by the Finance Department, i.e. in relation to the administration of the monthly payroll, pension details etc.

Confidential information relating to tenants and housing applications are held by the Housing Team on the computer system, the e-mail system and files in the relevant operational departments. Information on suppliers is held on file with the Finance Department. The Asset Management Team is also responsible for information on our tenants, as are our chosen Repairs and Maintenance partners.

Staff handling confidential information will ensure that this information remains confidential.

Members of staff, tenants or housing applicants will be offered an interview room or office to discuss with EPIC information of a personal or confidential nature, if requested.

The Company's Document Retention Policy will set out time periods for keeping and storing documentation covered under the Data Protection Act. After this period of time documentation will be destroyed in a confidential manner (i.e. shredding or by the use of a document destruction company).

Information held
Individuals will be made aware of the reasons why personal information is held on record and the people likely to have access to it through Privacy notices. Consent to disclose such information will be obtained from each individual at application stage (i.e. employment or housing) and they will be informed of the implications of giving their consent.

EPIC or its employees will not attempt to gain access to information that is not necessary for them to hold.

All information that is held will be relevant for the purpose for which it is required and will be kept securely.

Disclosure of information
Confidential information held will be passed to other organisations on a need-to-know basis and with an individual's consent unless there are exceptional circumstances. Exceptional circumstances include:

- Where there is clear evidence of fraud;
- To comply with the law;
- In connection with legal proceedings;
- Where it would be essential to enable EPIC to carry out its duties, e.g. where the health and safety of an individual would be at risk by not disclosing the information or where there is a legal requirement to do so.
- Anonymously for statistical or research purposes.

EPIC will also share tenant information with their chosen Repair and Maintenance partners in order to ensure all our properties are maintained to the highest standard.

Subject Access Requests
Individuals have a right under the Act to get a copy of the information that we hold on them, this is known as a right of subject access.

A subject access request must be responded to promptly and within no more than 40 days after it has been received. However, EPIC may ask for any information that will allow them to locate the information and confirm the individual's identity. EPIC will charge a fee of £10 for responding to a request to cover administration and postage. A subject access request must be made in writing either by letter or email. Alternatively, the form attached at appendix 1 can be used.

Subject access requests must be considered carefully to ensure that personal information about other individuals is not released without their consent. Further information and guidance on subject access requests can be found at the Information Commissioner's website at www.ico.gov.uk.

Subject Access Requests will be co-ordinated by the Executive Assistant.

Disposal of information
Where personal and confidential information is no longer required, it will be destroyed in line with our Document Retention Policy.

Confidentiality
Working in the Office
- Whether on the telephone or face to face you must verify a person's ID before you release information to them. Such checks can include, a customer password, last 3 digits of a national insurance number, last 3 digits of a telephone number, next of kin details, the last repair they reported etc. Do not use their Date of Birth on its own, however you can use it in conjunction with another check.

- Remember if you are still unsure, most house files should now have a photo of the tenant on file.
- If you are on the telephone to an organisation and want to verify that the person you are speaking to belongs to that organisation, end the call and tell them you will call them back on the details you have. Do not let them provide you with a number to call.
- Be aware of who else may be listening, particularly in areas open to the public, i.e. talking to tenants in Reception.
- Never disclose information like telephone numbers, addresses, bank details even if you believe the person to be genuine. If they want to check we have the correct information on file ask them to tell you what they believe it is and you can verify whether they are correct or not.
- At the end of the day get into a routine of clearing away all confidential information from your desk, locking desks and filing cabinets.
- Never leave confidential documents unattended. Place the documents in an envelope and place in your drawer.
- Always lock your workstation when you are away from your desk.

Taking Data and Files to Visits

- Only in exceptional circumstances should the whole file be taken to a visit. Staff should only take the items they need for the purpose of the visit.
- Do not leave documents unattended in cars.
- Do not leave documents unattended at the visit – ensure you keep them with you at all times.
- If you have to take a call during a visit and need to quote personal data, take yourself to somewhere more private.

Working from Home

- Staff must get authorisation from their line manager to take work home.
- Once authorisation is granted, identify which pieces of work will be taken home. Managers should encourage staff to limit the material they take home.
- Only in exceptional circumstances should the whole file be taken home.
- Do not read or process documents which include people's personal details on the train.
- Do not leave documents which include people's personal details unattended in cars.
- Store documents safely out of view at home and do not show them to other household members.

Storing, Sending and Securing Data

- Try to avoid storing personal data on memory sticks and laptops unless it is password protected.
- When sending personal data via email, ensure that it is sent either by a password protected document or using encryption.
- Do not discuss confidential information outside the office with interested third parties who have no particular right to know about the internal business of EPIC.
- Do not discuss confidential information internally. Be aware that we all have a responsibility only to discuss those matters of business that we are privy to within our own sections and departments with other members of staff where they have a legitimate right to know.

- If you are not certain that a person requesting their data is who they say they are (whether face to face or by phone) ensure that you carry out verification checks.

Loss or Unintentional Release of Data

- If you believe you have released data or lost data covered by the Data Protection Act, you must report it immediately to your line manager confirming:
    - The content you believe you lost / released.
    - How the incident occurred
    - Full details of what happened.
- A Working Party including at least one member of the Management Team and one Board Member will be set up to manage the breach and will:
    - Decide whether the breach means that customers need to be informed about the loss or release of their data.
    - Produce a recovery plan to include how the data can be located or stopped from further circulation.
    - Evaluate how the breach occurred and how such events can be prevented in the future.

Equality and Diversity Statement

In the interests of fairness we have moved away from relating unfair treatment with gender, age, disability etc. Instead we have adopted the following definition of unfair treatment:

> 'Giving someone preferential treatment over another without any proper justification.'

Monitoring and Reporting

Files will be monitored on an ongoing basis to ensure that they comply with this policy and the Document Retention Policy.

Responsibilities

It is the responsibility of the appropriate staff and board members to maintain confidentiality as set out within this policy. A breach of confidentiality is a serious offence.

It is the responsibility of all staff to inform a senior manager when they are made aware of a breach of confidentiality. The senior manager is responsible for taking appropriate action when made aware of a breach of confidentiality.

The Chief Executive and Executive Assistant are responsible for ensuring that board members comply with the policy.

Review Mechanism

The policy and procedure on confidentiality will be reviewed every 3 years to ensure that it is effective and complies with current good practice. A review will be carried out sooner should there be any changes to statutory requirements.

Complaints in respect of this Policy

All employees will be informed of this policy. Any complaints of breaches of confidentiality should be reported using EPIC's grievance or complaints procedures.

Training

All staff responsible for handling confidential employee information will be made aware of the Data Protection Act during their induction by being issued the policy. In addition, refresher training will be delivered to all staff.

Sources of Further Information

Further information on the Data Protection Act and how to implement it can be sought from the Executive Assistant or by contacting the Information Commissioner either by its website www.ico.gov.uk or by calling the helpline on 0303 123 1113. The helpline is open from 9am to 5pm, Monday to Friday.

Appendix 1

Data Protection Act 1998: Subject Access Request Form

Individuals have the right to access all personal data held on them, unless it relates to another person who has reasonably refused to consent to his or her personal data being disclosed or for another reason as detailed within the Data Protection Act 1998. All Requests will be complied with within 40 days and an administration fee of £10 is payable.

If you would like access to your personal data, please complete this form and either post it back or hand it in to the office, with the required fee.

Name:_____

Address:_____

_____

Contact Number:_____Email:_____

1. Please tick if you have ever been:

An employee ☐

A tenant ☐

A client ☐

Other ☐

Please State:_____

2. If we may have known you under a different name please state:

_____

3. If we find any information about you, would you like to:

- Have a look at it within our office, or ☐
- Have us send you a copy at given address. ☐

If you are only interested in obtaining certain information we hold please state which parts of information this is:

_____

_____

_____

_____

_____

_____

_____

_____

_____

4. I want to see the records you hold on me, and enclose the £10 fee (cheques should be made payable to EPIC Ltd):

Signed:……Date……

Please note:

- If the address you give above does not match the one in our records, we may have to ask you for additional identification.
- We will reply as quickly as we can. We aim to reply within 3 weeks, but we may take up to 40 days. If you have asked for a copy of the information we will send it to the address given above.
- We have information about members of our organisation, staff, volunteers, clients and people we think may be interested in our work. We don't keep this information once we no longer need it, so if you were in touch with us some time ago we may no longer have any information about you.
- We will show you everything we have about you, except that information that we may be allowed to hold back, which is also about someone else.