DOCUMENT TYPE: EXTERNAL

DATA PROTECTION POLICY

Author / Contact :

Fuad Al-Tawil
postie@teignenergycommunities.co.uk
01626 87 2721

Name, date and signature of Directors and Officers to confirm this has been read and accepted:

Fuad Al-Tawil (Director and Secretary)

Chloe' Beal (Finance & Membership officer)

Bob Hussey (Finance Director)

Helen Chessum (Publicity Officer)

Tony Cook (Publicity Director)

Jamie Burnham (Technology Director)

Contents

Section 1. Key details

This version of the policy was:

- Prepared by> Fuad Al-Tawil (Company Secretary)
- Approved annually before next AGM (last approval <TBD@ April'18 Board meeting>)
- Requires annual signature of Directors and officers to confirm it is up to date and read.
- Takes account of General Data Protection Regulation (**GDPR**) introduced 2018

Section 2. Introduction

Teign Energy Communities Ltd. (**TECs**) needs to gather and use certain information about individuals.

These can include members, stakeholders, suppliers, business contacts and other people the organisation has a relationship with or may need to contact.

This policy describes how this confidential data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

Section 3. Why this policy exists

This data protection policy ensures TECs:

- Complies with data protection law, including GDPR 2018 and follows good practice
- Protects the rights of officers, directors, members and partners
- Is open about how it stores and processes individuals' and other data
- Protects itself from the risks of a data breaches

Section 4. Data protection law

The Data Protection Act 1998 the 2018 GDPR European wide requirements describe how organisations must collect, handle and store confidential information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, confidential information must be collected and used transparently and fairly, stored safely and not disclosed unlawfully.

The Data Protection requirements include important principles. These say that confidential data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes with the full and clear consent from individuals
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Be processed in accordance with the rights of data subjects, i.e. including the right of the individual to access, correct and remove their personal data
7. Be protected in appropriate ways
8. Not be transferred to a country or area outside the European Union, unless this country or area also ensures an adequate level of protection and has the informed consent of the data subject.

Section 5. People, risks and responsibilities

5.1 Policy scope

This policy needs to be adhered to by the following groups when handling data held by TECs:

- All volunteers of TECs
- All contractors, suppliers and other people working on behalf of TECs

It applies to the following **confidential data** that the company holds relating to identifiable individuals or organisations (specifically Members, Volunteers, Stakeholders and Service Providers), even if that information technically falls outside of the Data Protection regulation. This covers:

- Names
- Dates of birth
- Postal addresses
- Email addresses
- Telephone numbers
- Members' bank account details (additional rules apply, these are highlighted in yellow)
- Members' investments and payments
- Contracts and Agreements
- Bid submissions
- Commercially sensitive correspondence/information

5.2 Data protection risks

This policy helps to protect TECs from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

5.3 Responsibilities

Anyone handling 'confidential data' will need to personally confirm that they have read and accepted the policy. This can be done as part of the AGM process where the policy will be reviewed/agreed.

Everyone who works for or with TECs has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles confidential data must ensure that it is handled and processed in line with this policy and data protection principles.

However, the following people have key areas of responsibility:

The **Board of Directors** is ultimately responsible for ensuring that TECs meets its legal obligations.

The **Company Secretary,** is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.

- Handling data protection questions from TECs volunteers/officers and anyone else covered by this policy.
- Dealing with requests from individuals to see the data TECs holds about them (also called 'data subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters.
- Reporting any breaches of unauthorised access of confidential data to the individual(s) effected and the Information Commissioner's Office (**ICO**) within 36hrs. Note that under the ICO rules, TECs is not required to register with the ICO.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with others individuals to ensure marketing initiatives abide by data protection principles.

Section 6. General guidelines to TECs Volunteers and Officers

The only people able to access data covered by this policy should be those who **need it for their work**.

Data **should not be shared informally**. When access to confidential information is required, this should be requested from the Company Secretary.

TECs will provide training/guidance to help those handling confidential data understand their responsibilities when handling this data.

Volunteers and anyone providing a service to TECs should keep all data secure, by taking sensible precautions and following the guidelines below.

- In particular, **strong individual passwords must be used** and they should never be shared, except where this is necessary to allow access to shared data.
- Confidential data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and securely disposed of.
- You **should request help** from the Company Secretary if you are unsure about any aspect of data protection.

Section 7. Acquiring data and informed consent

TECs must ensure that individuals are aware at the outset that their data is being processed, and that they understand:

- How the data is being used and where it is stored
- How to exercise their legal rights
- To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company. This requires affirmative action from individuals providing their confidential data, establishing a freely given, specific, informed and unambiguous consent.
- A copy of the terms under which the data is acquired/held as well as this policy must be made available on the company's website.

Section 8. Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Company Secretary.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see/access it. In particular membership application forms must never be copied and originals must be kept by the Secretary.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Ensure paper and printouts are **not left where unauthorised people could see them**, e.g. on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.
- When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
    - Data should be **protected by strong passwords** that are changed regularly. Files containing **Members' data** must additionally be encrypted.
    - If data is **stored on removable media** (like a memory stick, CD, DVD), these should be kept locked away securely when not being used.
    - Data should only be stored on **designated drives and servers**, Members' banking data must never be uploaded to a **cloud computing services**, this includes 3rd party servers such as MailChimp or e-mail servers, but excludes TECs' on-line banking service/server operated by the Co-op Bank.
    - Servers (including 3rd-party servers like MailChimp or e-mail servers) containing confidential data should be **sited in a secure location and have adequate access security**, away from where they can be accessed by others. The use of 'reputable' providers for such servers should therefore always be used.
    - Data should be **backed up frequently**. Those backups should be tested regularly, in line with TECs' standard processes. Two encrypted and synchronised copies should be kept of Members' data, one held by The Membership Officer, the other by the Company Secretary.

- Data should **never be saved directly** to laptops or other mobile computing devices like tablets or smart phones.
- All servers and computers containing data should be protected by **appropriate security software and a firewall**.

Section 9. Data use

Confidential data is of no value to TECs unless the business can make use of it. However, it is when confidential data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

When working with confidential data, ensure **the screens of computers are always locked** when left unattended.

Confidential data **should not be shared informally**. In particular, it should not be sent by email, which is not a secure form of communication, unless absolutely necessary and only if appropriately secured and agreed between the sender and recipient. Copies of these e-mails must be password protected if kept on a secure platform or deleted if kept on a Cloud Computing server (e.g. mail server/client).

Confidential data must always be **encrypted/pass-word protected before being transferred electronically**. The Company Secretary can explain how to send data internally and to authorised external contacts. In particular Members' Database and reference to Members banking information must be encrypted/pass-word protected at all times and only shared by individuals identified in Section 8 .

Confidential data should **never be transferred outside of the European Union without the consent of data subjects**.

Section 10. Data accuracy

The law requires TECs to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that data is accurate, the greater the effort TECs should put into ensuring its accuracy.

It is the responsibility of all volunteers, officers and service providers who work with TECs data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data is held in **as few places as necessary**. Do not create any unnecessary additional data sets.
- **Take every opportunity to ensure data is updated.** Follow the regular operational processes.
- TECs will make it **easy for Members to update the information** TECs holds about them, except for their banking details. For instance, via the MailChimp server.
- Data should be **updated as inaccuracies are discovered**. For instance, if a Member can no longer be reached on their stored e-mail, this should be addressed immediately.

Section 11. Subject access requests

All individuals who are the subject of confidential data held by TECs are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the company requesting this information, this is called a **subject access request**.

Subject access requests from individuals should be made by email, addressed to the Company Secretary.

The Company Secretary will always verify the identity of anyone making a subject access request before handing over any information.

Section 12. Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows confidential data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, TECs will disclose requested data. However, the Company Secretary will ensure the request is legitimate, seeking assistance from the Board and from the company's legal advisers where necessary.

Section 13. Complaints Procedure

In the first instance any concerns relating to Data Protection should be reported to the Company Secretary. If the concern cannot be resolved or a complaint needs to be made, the ICO should be contacted.

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/complaints/