Introduction

Epworth Town Council needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.
This policy describes how this personal data must be collected, handled and stored to meet the Town Council's data protection standards – and to comply with the law.

Why this Policy exists

This data protection policy ensures that Epworth Town Council;

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection Law

The Data Protection Act 1998 describes how organisations – which includes Epworth Town Council- must collect, handle and store personal information.
These rules apply regardless of whether data is stored electronically, on paper or in some other form.
To comply with the law, personal information must be collected and used fairly, stored safely, and not disclosed unlawfully.
The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
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. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People Risks and Responsibilities

Policy Scope

This policy applies to:

- All Councillors, staff and volunteers of Epworth Town Council
- All contractors, suppliers and other people working on behalf of Epworth Town Council

It applies to all data that Epworth Town Council holds relating to identifiable individuals, even if that information technically falls outside of the Data protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers

- …plus any other information relating to individuals

Data Protection Risks

This policy aims to protect Epworth Town Council from data security risks, including:

- **Breaches of confidentiality**.
- **Failing to offer choice**. (All individuals should be free, having regard to the statutory guidelines, to choose how Epworth Town Council uses data by statute relating to them
- **Reputational damage.**

Responsibilities.

Although Epworth Town council is ultimately responsible for ensuring that the Council and everyone who works for or on its behalf (whether that be on a voluntary or employed basis) meets the obligations imposed under the Act,

Everyone who works for or with Epworth Town Council has some responsibility for ensuring data is collected, stored and handled appropriately. For example.

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

In addition,

The clerk will be responsible for:

- Keeping the Council updated about its data protection responsibilities, risks and issues
- Ensuring that all data protection procedures and related policies, are reviewed annually, in line with an agreed schedule.
- Arrange appropriate data protection training and advice for all those covered by this policy.
- Handling data protection questions from Councillors, staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data Epworth Town Council holds about them (also called “A subject access request”).
- Ensuring that Full council checks and approves any contracts or agreements with third parties that may handle the Town Council’s sensitive data on its behalf.
- 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.
- Obtaining information about any third-party services the Town Council is considering using to store or process data. For instance, cloud computing services.
- Ensuring that a suitable data protection statement is attached to all communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.

General Guidelines

- 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 requested, enquiries should be made of the Town Clerk in the first instance.
- Epworth Town Council will ensure that suitable training is provided for the clerk and Councillors to ensure that they understand their respective responsibilities when handling data.
- The Clerk will ensure as far as possible that all data is kept secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and should be changed regularly. Passwords should never be shared.
- Personal data should not be disclosed to unauthorised people, either within Epworth Town Council or externally.
- Data held should be kept updated and regularly reviewed in accordance with the document retention schedule and updated. If no longer required, it should be deleted or securely disposed of.
- The clerk should request help from the personnel committee in the first instance if unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Town Clerk in the first instance.
When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.
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.
- The clerk should make sure 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 hacking attempts.

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing service.**
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the “Town Councils” back up procedure.
- Data should **never be saved dir**ectly to laptops or other mobile devices like tablets or smart phones.

- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data use

Personal data is of no value to "Epworth Town Council" unless it can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by e-mail, as this form of communication is not secure.
- Data should be **encrypted before being transferred electronically**. Procedures should be put in place to send personal data safely and securely to authorised external contacts.
- Employees **should not save copies of personal data to their own computers**.

It is the responsibility of the Clerk to take all reasonable steps to ensure data held is kept as accurate and up to date as possible.

- Epworth Town Council will make it **easy for data subjects to update any information** Epworth Town Council holds about them by publishing this policy (i.e. on the website etc.) accompanied by the process by which they can make a request to update.
- Data should be **updated if and when any inaccuracies are discovered**. For instance, when it is discovered that an individual can no longer be reached on their stored telephone number, that number should be removed from the Councils database or list.

Subject access requests

All individuals who are the subject of personal data held by Epworth Town Council are entitled to:

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

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

Subject access requests from individuals must be made in writing and addressed to the Clerk. Such applications may be sent by e mail to epworth.council@btconnect.com by post to Epworth Town Council, Cemetery Lodge, Burnham Road, Epworth, Doncaster, DN9 1BY or hand delivered. However it is possible to make such requests via social media and therefore both Councillors and the clerk need to be aware of this and refer any such requests to the Clerk without delay.

Proper requests received will be acknowledged within 10 working days of receipt. The Clerk will verify the identity of anyone making a subject access request before identifying all relevant information to be disclosed.

Individuals may be charged £10 per subject access request (the maximum charge permitted by law) for supplying copies of documents.
The clerk will always verify the identity of anyone making a subject access request before handing over any information. The clerk will ensure that the disclosure is made within the statutory time period of 40 days from the date of receipt of the initial request.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act provides that personal data must be disclosed to law enforcement agencies without the consent of the data subject.
In these situations Epworth Town Council is under a legal obligation to disclose the requested data, however, the clerk will ensure the request is legitimate, seeking assistance and advice as and when it is considered necessary and appropriate to do so.

Providing information

Epworth Town Council aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used.
- How to exercise their rights in respect of that data.

In order to meet these aims Epworth Town Council has a privacy statement, setting out how data relating to individuals is used by the Town Council, which is available on the Epworth Town Council web-site. Copies of the privacy statement are also available on request.

DM/CMMAR 2017

.