Data Protection Policy

Overview

Details

- Policy prepared by: Linda Hedley
- Approved by Council on: 12th September 2017
- Policy became operational on: 13th September 2017
- Next review date: Before end 2018

Introduction

Sellindge Parish Council needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the council 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 council's data protection standards – and comply with the law.

Why this policy exists

This data protection policy ensures Sellindge Parish Council:

- Complies with data protection law and follows good practice
- Protects the rights of staff and all other business associates
- Is open about how it stores and processes individuals data
- Protects itself from the risk of data breach

Data protection law

The data Protection Act 1998 describes how organisations – including Sellindge Parish Council, must collect, handle and store personal information.

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

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 state 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, unless that country or territory also ensures an adequate level of protection

People, risks and responsibilities

Policy Scope

This policy applies to:

- The principal office of Sellindge Parish Council
- All other facilities run by Sellindge Parish Council
- All staff and volunteers of Sellindge Parish Council
- All contractors, suppliers and other organisations working with or on behalf of Sellindge Parish Council

It applies to all data the council holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1988. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Plus any other information relating to individuals

Data protection risks

This policy helps to protect Sellindge Parish Council from very real data security risks, including:

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

Responsibilities

Everyone who works for Sellindge Parish Council has some responsibility for ensuring data is collected stored and handled appropriately.

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

However, there are certain areas of key responsibility:

- The duly elected members working in conjunction with the Parish Clerk are ultimately responsible for ensuring that Sellindge Parish Council]meets its legal obligations.

- The officer in charge of the protection of data is responsible for:

    - Keeping members/town/parish clerk updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection and related policies, in line with agreed procedures.
    - Arranging data protection training and advice for people covered by this policy,
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data the council holds about them (called subject access requests)
    - Checking and approving any contracts or agreements with third parties that may handle the council's sensitive data.
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets.
    - Where necessary, working with other officers to ensure marketing initiatives abide by data protection principles.

- The officer in charge of IT is responsible for:

    - 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 council is using or considering using to store or process data. For example, cloud computing services.

General officer 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 required, officers can request it from their line manager.
- The Council will provide training to all employees to help them understand their responsibilities when handling data.

- Officers should keep all data secure, by taking sensible precautions and following the guidelines below
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the council or externally.
- Data should be regularly reviewed and updated if it is found to be out of date or if no longer required it should be deleted and securely disposed of.
- Officers should request help from their line manager or the data protection officer if they are 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 officers responsible for data protection and IT.

Data stored on paper

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.
- Officers should make sure paper and printouts are not left where unauthorised people could see them, like a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

Data stored electronically

When data is stored electronically, it must be protected form unauthorised access, accidental deletion and malicious hacking attempts.

- Data should be protected by strong passwords that are changed regularly and never shared between officers.
- If data is stored on removable media (like a CD, DVD or memory stick), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives or servers, and should only be uploaded to approved cloud/server computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with standard backup procedures.

- Data should never be saved directly to laptops or other mobile devices like memory sticks, tablets or smartphones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of ne value to the 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, officers should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular it should not be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically.
- Personal data should never ne transferred outside of the European Economic Area.
- Offices should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data accuracy

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

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

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

- Data will be held in as few places as necessary. Officers should not create any unnecessary additional data sets.
- Officers should take every opportunity to ensure data is updated. For instance by confirming customer or supplier details when they call.
- The council will make it easy for data subjects to update the information the council holds about them. For instance via the council website.
- Data should be updated as inaccuracies are discovered. For example, if a contact can no longer be reached on their stored details, then they should be removed from the data base.

Subject access requests

All individuals who are subject to personal data held by the council are entitled to:

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

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

Subject to access requests from individuals should be made in writing, address to the responsible officer. The responsible officer can supply a standard request form, although individuals do not have to use this.

Individuals can be charges up to £10 per subject access request. The responsible officer will aim to provide the relevant data within 14 days.

The responsible officer will always verify the identity of anyone making a subject to access request before handing over any information.

Disclosing data for any other reasons

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

Under these circumstances, the council will disclose the requested data. However the responsible officer will ensure the request is legitimate, seeking assistance from the Parish Clerk in conjunction with the Leader of the Council and from the Council's legal advisers where necessary.