BLYTH TOWN COUNCIL

DATA PROTECTION POLICY

INTRODUCTION

Blyth Town 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 to comply with the law.

WHY THIS POLICY EXISTS

This data protection policy ensures Blyth Town Council:

- Complies with data protection law and follow 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 - including Blyth Town Council - must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on 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 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

Our Commitment

We are committed to:

- ensuring that we comply with the eight data protection principles, as listed above
- meeting our legal obligations as laid down by the Data Protection Act 1998
- ensuring that data is collected and used fairly and lawfully
- processing personal data only in order to meet our operational needs or fulfil legal requirements
- taking steps to ensure that personal data is up to date and accurate
- establishing appropriate retention periods for personal data
- ensuring that data subjects' rights can be appropriately exercised
- providing adequate security measures to protect personal data
- ensuring that Town Clerk is responsible for data protection compliance and provides a point of contact for all data protection issues
- ensuring that all staff are made aware of good practice in data protection
- providing adequate training for all staff responsible for personal data
- ensuring that everyone handling personal data knows where to find further guidance
- ensuring that queries about data protection, internal and external to the Council, is dealt with effectively and promptly
- regularly reviewing data protection procedures and guidelines within the Council

The Town Council has registered the type of data they process with the Information Commissioner's Office. The registration is renewed on a 3 yearly basis or when the business needs change.
The registration reference is ZA065709.

Although we treat all information the same, in accordance with the Act, there is stronger legal protection for more sensitive information, such as:

- ethnic background
- political opinions
- religious beliefs
- health
- sexual health
- criminal records.
-

PEOPLE, RISKS AND RESPONSIBILITIES

This policy applies to:

- All members, staff and associates of **Blyth Town Council**
- All contractors, suppliers and other people working on behalf of Blyth Town Council
- It applies to all data that the 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 helps to protect Blyth Town Council 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 Council uses data relating to them.

- **Reputational damage.** For instance, the council could suffer if hackers successfully gained access to sensitive data.

Responsibilities

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

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

However, these people have key areas of responsibility:

- The Town Council is ultimately responsible for ensuring that Blyth Town Council meets its legal obligations.
- The **Town Clerk,** is responsible for:
  - Keeping the staff updated about data protection responsibilities, risks and issues.
  - Reviewing all data protection procedures and related policies, regularly.
  - Arranging data protection training and advice for the 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 Blyth Town Council holds about them (also 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 like newspapers.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.
- The **IT Consultant,** 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 considering using

to store or process data. For instance, cloud computing services.

GENERAL STAFF 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, employees can request it from their line managers.
- **Blyth Town Council will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees 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. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from the Town Clerk 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 Town Clerk initially.

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**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like 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 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 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 the Council's standard backup procedures.
- Data should **never be saved directly** 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 Blyth Town Council unless the business can make use of it. However, it is when data relating to a person's own circumstances 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 email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT consultant can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area**.
- Employees **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 Blyth Town Council to take reasonable steps to ensure data is kept accurate and up to date.

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

It is the responsibility of all employees 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**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.

- Blyth Town Council will make it **easy for data subjects to update the information** Blyth Town Council holds about them. For instance, via the website.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database or any related list.

SUBJECT ACCESS REQUESTS

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

- Ask **what information** the 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 the Council is **meeting its data protection obligations**.

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

Subject access requests from individuals should be made by email, addressed to the Town Clerk at info@blythtowncouncil.gov.uk.

This request can also be made by letter by writing to:

The Town Clerk
Blyth Town Council
Arms Evertyne House
Quay Road
Blyth
NE24 2AS

How much it costs

Some organisations may charge individuals for providing the information. The cost is usually no more than £10 but it can be more e.g. if the information is difficult to obtain because of its volume and how stored. This will be made clear when the application for information has been received. In our case we will waive the minimum charge where the information is readily available.

The Town Clerk will aim to provide the relevant data within 14 days.

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

DISCLOSING DATA FOR 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, Blyth Town Council will disclose requested data. However, the Town Clerk will ensure the request is legitimate, seeking assurances where necessary.

PROVIDING INFORMATION

Blyth 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

To these ends, the Council has a privacy statement, setting out how data relating to individuals is used by the council.

The approved version of this document will be placed on the Council's website.