BLYTH TOWN COUNCIL

DATA PROTECTION POLICY

Version	2
Author	**H Jenner**
Date approved	
Previous versions	

Contents

Introduction

Blyth Town Council needs to gather and use certain information about individuals.

These can include residents, 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.

This data protection policy ensures Blyth 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

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.

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.

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

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

The General Privacy Notice sets out how data relating to individuals is used by the council.

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:
    - Acting as the Data Protection Officer and the point of contact for all data protection matters.
    - Keeping the staff updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, regularly.
    - Arranging regular training to ensure all staff and members are trained on data protection principles and practices.
    - Arranging regular data audits to identify what personal data is held, how it is used and make sure it is processed lawfully. Maintaining this data in an Information Asset Register.
    - Handling data protection questions from staff and anyone else covered by this policy effectively and promptly, within legal timescales as applicable.
    - 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.

♦ **All staff** are responsible for:

- Ensuring they are aware of good practice in data protection.
- Complying with training and guidance received as part of their role.
- Reporting breaches of data protection immediately to the Town Clerk
- Proactively seeking further guidance and requesting help from the Town Clerk if they are unsure about any aspect of data protection.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

Data Use and Processing

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

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.

♦ Personal data should not be disclosed to unauthorised people, either

within the Council or externally.

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 Backups

Blyth Town Council is committed to ensuring its IT Systems are secure, Town Council data and systems are protected, and are only accessed by authorised users. The Data storage process has been set up to ensure secured copies of data are accessible in case of disaster recovery with mechanisms in place on and off site to facilitate this.

A system is in place on site relating to the backing up and storage of

existing council electronic data. This includes:

- A live network storage device that has two disk drives. The first drive holds the data that is accessible by the staff. The second holds a duplicate that is copied each time data is written in case the first drive fails. Staff can only access the first drive to ensure data is not altered on the second drive.
- A backup device (also with two disk drives) that copies the entire contents of the first device weekly and is stored in a directory with the current date. Each month a copy of the latest weekly backup is archived in a directory with the current months date. Both the network storage device and the backup device are housed in a locked data cabinet in the Town Council storage room.
- An encrypted connection from the IT Council PC on site that once per week uploads any incremental changes to a server rented for the sole use of the Council at a secure data exchange in London run by Rackspace Ltd. Access to the encrypted connection is via a PGP key that is stored on a USB disk in a locked cabinet at the Council offices. Data cannot be downloaded without the PGP key and has to be done from the IT Council PC or from a secured PC at the IT Consultants office. The IT Consultants do not hold the PGP key; this is to ensure that the Council knows when the external server is being accessed offsite.

The above processes are checked weekly by the IT Consultant to confirm that all backups have run as required. If there any failures, these are resolved at that point by the IT Consultant.

In addition, a manual quarterly backup is taken from the live storage device to the IT Council PC.

Security on the devices is as follows;

- The two storage devices (Live and Backup) require a username and password (random characters) to access the backups. The devices are stored in a locked data cabinet that is in the Council Store room that should remain locked when not in use.
- The IT Council PC is secured with a username and password that is greater than 12 digits and includes letters and numbers.
- The encrypted connection can only be access with the PGP key. The details for the PGP key are stored on a USB drive in a locked cabinet in the council offices.
- No physical access is possible to the public as the offices require an electronic fob for the building and for the actual offices. CCTV camera is onsite to monitor physical access.

- The external server is held at Rackspace in a secure data centre with CCTV and electronic locking on all access points. The server is only accessible via secure SSH or secure FTP using the encrypted PGP code. It was agreed by the council that Rackspace would be used due to their reputation for hosting a secure network.

Full details can be found in the related internal backup system procedures document currently in use including passwords to access on and offsite data. For security purposes this document must remain on site.

Data Sharing and Disclosures

Data Sharing

The council will on occasion share data sets or types of data routinely for established purposes.

Written Data Sharing Agreements between the council and the other organisation(s) govern such routine sharing. DSAs ensure that personal data remains adequately protected with proper security.

Copies of DSAs are stored in the Information Asset Register. They should be signed by the relevant Officer creating such agreements.

The Data Protection Officer shall be notified of the creation of, changes made to or terminations of any DSA.

Freedom of Information

Blyth Town Council abides by the Freedom of Information Act 2000 which gives a general right of access to all types of information held by public authorities.

Any person who makes a request to a public authority for information must be informed whether the public authority holds that information and, subject to exemptions, supplied with that information.

All freedom of information requests should be submitted via email to info@blythtowncouncil.gov.uk and should give a clear indication of the information being requested.

See the Freedom of Information Policy for more information.

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 and ask how to gain access to it. This is called a subject access request or SAR.

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

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

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

See the Subject Access Request Policy for further information.

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.

Data Accuracy And Updates

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.

Blyth Town Council will make it easy for data subjects to update the information Blyth Town Council holds about them.

- 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 in accordance with disposal principles.
- 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.
- 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.

Other relevant policies:

- Subject Access Request Policy
- General Privacy Notice

- CCTV Procedure