Penybont & Landegley Community Council

Security & Confidentiality Policy

1. Scope

Penybont & Llandegley Community Council aims to ensure that the procedure it adopts in the utilisation of confidential information complies with the highest ethical standards and fully endorses and adheres to the eight principles of the Data Protection Act
1998 and the Equality act 2010 and the GENERAL DATA PROTECTION REGULATIONS (GDPR) Legislation of 2018.

Staff and Councillors strive to handle information in compliance with the following:

- Data Protection Act 1998
- Rehabilitation of Offenders Act 1974
- Human Rights Act 1998
- GENERAL DATA PROTECTION REGULATIONS (GDPR) Legislation 2018
- Freedom of Information Act (see separate policy)

These procedures foster a relationship of trust with individuals and/or their representatives, employees and third-party agencies and organisations.

All parts of this document relate to both Councillors and Staff.

2. Principles

Penybont & Llandegley Community Council is the Data Controller.

The General Data Protection Regulations list the data protection principles in the following terms:

- **1. Fair and lawful**
  Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
  a) At least one of the conditions in Schedule 2 is met, and
  b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

- **2. Specific for its purpose**
  Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes unless prior consent from the individual is received.

- **3.** By adequate and only for what is needed.
  Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- **4. By Keeping personal data accurate and up to date**
  Personal data shall be accurate and, where necessary, kept up to date.

- **5. Not kept longer than needed**
  Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

- **6. Take into account people's rights**
  Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Individuals have general right of access to their personal information which is processed by the Town Council. They have the right to:

  i. To have a copy of the information
  ii. To stop processing where this is likely to cause distress
  iii. To have information rectified, blocked or erased

- **7. Kept safe and secure**
  Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- **8. Not be transferred outside the EEA**
  Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3. Information Gathering

All information gathered in the course of discussion with an individual, whether or not a third party is present, should be relevant and regarded as confidential. No information about an individual should be passed on to another party or organisation without the permission of the individual concerned unless in lawful circumstances.

Individuals will be informed of the relevance and purpose of the information gathered and will have the opportunity to evaluate this process and comment on the service provided. They will have the opportunity to remain anonymous.

The individual concerned must be consulted and give consent for information that may be made available to another party or organisation. Any limitations with regard to confidentiality should be made very clear to the individual or member of staff at the earliest stage. In situations where the purpose of the transfer of information is to the benefit of the individual, their approval should be sought in a balanced and unbiased way.

All information will be accurate and up to date including referrals made and outcomes in terms of employment and training. Copies of documents and records produced by the organisation referring to the individual will be made available if requested.

In exceptional circumstances, where for example an individual may be a potential danger to staff, to a minor or to themselves, the staff member concerned must refer the matter to the Town Clerk who will consider the matter and decide on any action.

Where a breach of confidentiality is considered necessary then legal advice must be sought.

4. Security of Information

All records about an individual remain the property of that individual. All such information must remain confidential and be up to date and be stored in a secure environment.

Councillors and staff must be aware of the existence of the type of records kept on individuals e.g. forms, computer databases, personal development plans, certificates, personnel records etc., and be aware of the content of such records.

Staff and Councillors will be aware that confidentiality of information is very important, and that breaching confidentiality could lead to disciplinary procedures being implemented.

As a clear guide – if a matter was discussed in a formal Council or Committee meeting at which the public could have attended then matters discussed are not considered confidential. If a matter was discussed in a formal Council or Committee meeting at which the public would not have attended, then matters discussed are considered to be confidential.

Written records will be stored in appropriate filing cabinets or store cupboards which will be kept locked. Computer records containing personal information will have password protection, creating restrictions on workstation access and file access (two levels). Back up will be securely stored.

Individuals or other visitors to premises used by the Community Council will not be allowed to use computers that have access to client or staff personal information unless they are properly supervised. Similarly, no such person will be allowed access to the filing cabinets or store cupboards containing such information.

When leaving any such premises, staff must ensure all filing cabinets and store cupboards containing personal information are properly secured and all computers correctly closed down.

Anyone who has any enquiries or complaints regarding Data Protection can contact the Council who has approved this policy, in writing.

Computer Security:

The following measures have been put in place:

- Firewall and virus-checking installed on computer.

- Operating system set up to receive automatic updates.
- Download the latest patches or security updates, which should cover vulnerabilities to computer automatically
- Only allow Members access to the information they need to carry out their work and do not share passwords.
- Regular back-ups of the information on your computer system taken and kept in a separate place.
- All personal information will be removed before disposing of old computers (by using technology or destroying the hard disk).
- Anti-spyware tool installed. Spyware is the generic name given to programs that are designed to secretly monitor your activities on your computer. Spyware can be unwittingly installed within other file and program downloads, and their use is often malicious. They can capture passwords, banking credentials and credit card details, then relay them back to fraudsters. Anti-spyware helps to monitor and protect your computer from spyware threats, and it is often free to use and update.

Using Emails Securely:

The following guidance has been issued:

- Before sending consider whether the content of the email should be encrypted, or password protected.
- Take care when typing in the name of the recipient; some email software will suggest similar addresses that have been used before. If you have previously emailed several people whose name or address starts the same way. Make sure to choose the right address before clicking send.
- To send an email to a recipient without revealing their address to other recipients, make sure blind carbon copy (bcc) is used, in place of carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.
- Take care when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.

  To send a sensitive email from a secure server to an insecure recipient, security will be threatened. Check that the recipient's arrangements are secure enough before sending your message

Other Security:

- Confidential paper waste will be shredded/burnt
- Physical security of premises considered

5. Disclosure

We aim to provide the best possible opportunity for our citizens and staff. If you have any particular requirements that will improve our services, please let us know as soon as possible and we will endeavour to make reasonable changes.

Your right for that information to remain confidential will not be jeopardized and will be treated with extreme urgency and respect. Where possible we will make reasonable adjustment to accommodate need.

6. Data Breaches

Every effort is taken to make sure the correct procedures are in place to detect, report and investigate a personal data breach.

Penybont & Llandegley Community Council is required to notify the ICO (and possibly some other bodies) when a personal data breach is suffered. Notification will take place where a breach is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, monetary loss, loss of confidentiality or any other significant economic or social disadvantage. Breaches must be reported to the ICO within 72 hours.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, Penybont & Llandegley Community Council will also have to notify those concerned directly in most cases.

Procedures are in place to effectively detect, report and
investigate a personal data breach. Penybont & Llandegley Community Council may wish to assess the types of personal data it holds and document where you would be required to notify the ICO or affected individuals if a breach occurred.

7. Data Protection Officer

Penybont & Llandegley Community Council will designate someone to take responsibility for data protection compliance and assess where this role will sit within our organisational structure and governance arrangements. The requirement is to formally designate a Data Protection Officer (DPO) as a public authority.

8. **Termination of Membership/Employment**

All Staff commit to adhering to this policy following the termination of individual employment, All members commit to adhering to this policy following their completion of service until the end of their expected term of office in May of a Town Council election year.

9. Impact Assessment

A data impact assessment will be carried out every 12 months to ensure compliancy with GDPR and the Council's policies.

Draft Prepared	14th March 2018
Draft Approved	1oth July 2018