Appleby-in-Westmorland Town Council

Data Protection Policy

GENERAL STATEMENT

1. Appleby-in-Westmorland Town Council recognises and accepts its responsibility to comply with the General Data Protection Regulations 2018 which regulates the use of any personal data. The purpose of this policy is to ensure the confidentiality and lawful and correct treatment of personal data. To this end, the Council fully endorses and adheres to the principles of data protection as detailed in the General Data Protection Regulations 2018 and any subsequent amendments.

2. Personal data will be:

   - processed fairly and lawfully
   - obtained only for lawful and specific purpose(s)
   - adequate, relevant and not excessive in relation to the purpose for which it was collected
   - accurate and when necessary kept up to date
   - kept for no longer than is necessary for the purpose for which it was collected
   - processed in accordance with the rights of the data subjects
   - kept securely
   - held and only used within the European Economic Area

3. Personal data is defined in the Regulations as "data which relates to a living individual who can be identified:-
   - from those data; or
   - from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual".

DATA COLLECTION.

When collecting personal data the Council will ensure that people know:

a) Who we are
b) What the data will be used for
c) To whom it will be disclosed

We will ensure that no more data is collected than that which is required for the purpose for which it is being collected.

DATA HANDLING

When handling, collecting, processing or storing personal data the Council will ensure that;

a) All personal data is both accurate and up to date
b) Errors are corrected effectively and promptly
c) The data is destroyed/deleted when it is no longer needed
d) The personal data is kept secure at all times (protecting from unauthorised disclosure or access)
e) The Regulations are considered when setting up new systems or when considering use of the data for a new purpose. Note that this may require registration with the Information Commissioner's Office
f) written contracts are used when external bodies process/handle the data explicitly specifying the above requirements with respect to the data

Members or employees of the Council will not:

a) Access personal data that is not needed for our work
b) Use the data for any purpose it was not explicitly obtained for
c) Keep data that would embarrass or damage the Council if disclosed (eg; via a subject access request – see below)
d) Transfer personal data outside of the European Economic Area unless you are certain you are entitled to or consent from the individual concerned has been obtained
e) Store/process/handle sensitive personal data (see below) unless you are certain you are entitles to or consent from the individual concerned has been obtained. 'Sensitive data' means data pertaining to: racial or ethnic origin; religious or similar beliefs; trade union membership; physical or mental health or sexual; political opinions; criminal offences. This data may only be held in strictly defined situations or where explicit consent has been obtained.

SUBJECT ACCESS

Individuals who the data relates to have various rights:

a) To receive on request details of the processes relating to themselves. This includes any information about themselves including information regarding the source of the data and about the logic of certain "fully automated decisions"
b) To have any inaccurate data corrected or removed in a timely fashion
c) In certain circumstances to stop processing likely to cause "substantial damage or substantial distress"
d) To prevent their data being used for advertising or marketing
e) not to be subject to certain "fully automated decisions" if they significantly affect him/her

When a subject access request is received, the Council will respond within the required timescales as defined in the Regulations.

A fee to cover photocopying and postage will be charged to the person requesting the personal information. This fee will be agreed by the Council and amended in line with inflation from time to time.

INFORMATION SECURITY

The Council will ensure that all information whether stored electronically or as paper records will be stored securely to ensure that;

a) Only authorised people can access, alter, disclose or destroy any personal data
b) Councillors and employees of the Council only act within the scope of their authority
c) If personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individual concerned

All personal information held by the Council will be kept in a secure location and not available for public access.

All such data stored on a computer will be password protected.

Personal data will be monitored on a regular basis and shredded or deleted once it has served its purpose, is not needed any more or is out of date. Except in exceptional circumstances and as agreed by Council, personal data will be kept for no longer than three years.

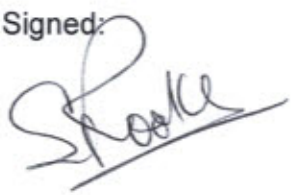
Councillors and employees must be aware that when complaints or queries are made, they must remain confidential unless the subject gives permission otherwise. When handling personal data, this must also remain confidential.

POLICY REVIEW

This Data Protection Policy will be reviewed annually by Appleby-in-Westmorland Town Council at the Council Meeting held in January.

This policy has been agreed and approved by Appleby-in-Westmorland Town Council.

Signed:



Cllr Rooke
Mayor (Appleby-in-Westmorland Town Council)

Dated: Wednesday 21st November 2018