



**AMBER VALLEY
BOROUGH COUNCIL**

DATA PROTECTION POLICY

This is a statement of the data protection policy adopted by Amber Valley Borough Council (“the Council”).

The Council needs to collect and use certain types of personal data about people with whom it deals in order to operate. These may include current, past and prospective employees, tenants, customers, residents, suppliers, voters, agents etc and others with whom it communicates. In addition, it may occasionally be required by law to collect and use certain types of information of this kind to comply with the requirements of the law itself or other governmental authorities or bodies. Such personal information must be dealt with properly however collected, recorded or used – whether on paper, in a computer, or on other material – and there are safeguards to ensure this in the Data Protection Act 1998 with which the Council must comply.

The Council regards the lawful and correct treatment of personal information by its employees and agents as very important to successful operations, and to maintaining the confidence of those with whom it deals.

To this end, the Council fully endorses, and adheres to, the Principles of data protection as enumerated in the Data Protection Act 1998.

Specifically, the Principles require that personal data:

1. shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;
2. 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;
3. shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
4. shall be accurate and, where necessary, kept up to date;
5. shall not be kept for longer than is necessary for that purpose or those purposes;
6. shall be processed in accordance with the rights of data subjects under the Act;

and that:

7. 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. 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.

Therefore, the Council will, through appropriate management, and strict application of criteria and controls:

- observe fully conditions regarding the collection and use of information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of information used;
- apply strict checks to determine the length of time information is held;
- ensure that the rights of people about whom information is held can be fully exercised under the Act. (These include: the right to be informed that processing is being undertaken; the right of access to one's personal information; the right to prevent processing in certain circumstances; the right to have wrong information corrected, blocked, rectified or erased);
- take appropriate technical and organisational security measures to safeguard personal information;
- ensure that personal information is not transferred abroad without suitable safeguards.

In addition, the Council will ensure that: -

- there is someone with specific responsibility for data protection in the organisation. Currently, the Nominated Person is Anthony Augustine Mark.
- everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- everyone managing and handling personal information is appropriately trained to do so;
- everyone managing and handling personal information is appropriately supervised;
- anybody wanting to make enquiries about handling personal information knows what to do;
- queries about handling personal information are promptly and courteously dealt with;
- methods of handling personal information are clearly described;
- a regular review is made by Business Unit managers of the way personal information is managed;
- methods of handling personal information are regularly assessed and evaluated by Business Unit Managers;
- performance with handling personal information is regularly assessed and evaluated by Business Unit Managers.

Non-Compliance with the Act

To protect the Council and the staff of the Council from inadvertent breaching of the Act, general guidelines will be issued to all departments.

Any member of staff deliberately breaching the Council’s Data Protection Policy may be subject to disciplinary procedures.

Role of Elected Members

This Act affects elected Members in three different capacities:

- a) as members of a committee or the Council and, therefore, subject to the same rights, responsibilities and penalties as employees of the Council;
- b) acting on behalf of a member of the public; and
- c) personally when the rights of data subjects apply.

The Data Protection Act and this Policy Statement do not change any duties, rights or responsibilities imposed by any other enactment.

With regard to a) and c), the rules which apply to staff also apply to elected Members of the Council.

Members of the Council will only seek access to data when knowledge of such data is essential for them to undertake their Council responsibilities or where the data subject has authorised the access (b above).

Advice and Training

The Council has appointed officers, as necessary, to meet the aims and requirements of the Act. As far as practicable, the Council will provide training for employees to comply with this policy.

Issue and Review

A copy of this statement shall be brought to the attention of all employees. It will be reviewed from time to time.

Authorised by

Date

Signed by

Date