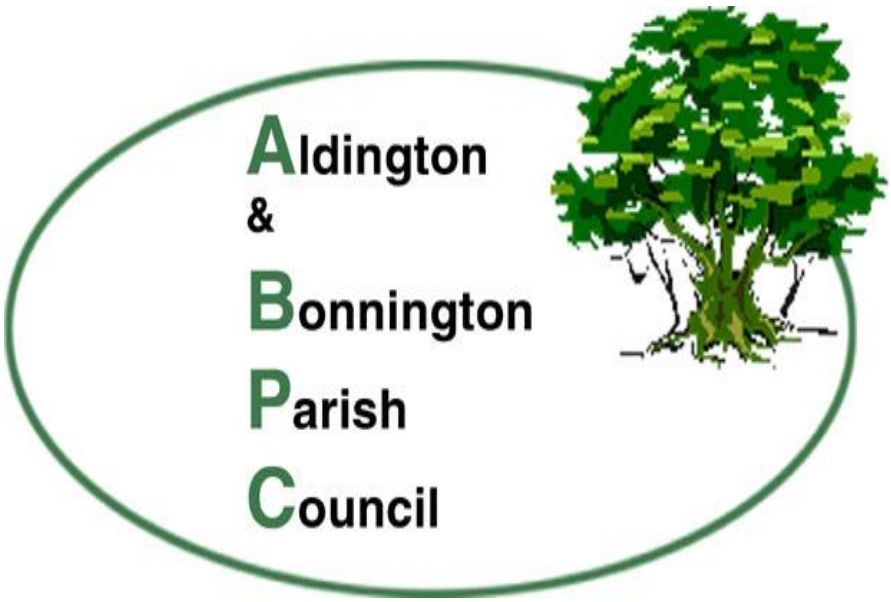
Data Protection
and
Information Security Policy.



Adopted January 2015.

Aldington and Bonnington Parish Council
Data Protection and Information Security Policy.

Aldington and Bonnington Parish Council recognises its responsibility to comply with the Data Protection Act 1998 which regulates the use of any personal data.

The purpose of the 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 Data Protection Act 1998 and any subsequent amendments.

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 where 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.

Personal data is defined in the Act, 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:-

1. who we are,
2. what the data will be used for,
3. 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:

1. all personal data is both accurate and up to date,
2. errors are corrected effectively and promptly,
3. the data is deleted/destroyed when it is no longer needed,
4. the personal data is kept secure and at all times (protecting from unauthorised disclosure or access),

5. the Data Protection Act is considered when setting up new systems or when considering use of the data for a new purpose.
6. 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:

1. access personal data that is not needed for our work,
2. use the data for any purposes it was not explicitly obtained for,
3. keep data that would embarrass or damage the Council if disclosed (eg. Via a subject access request – see below)
4. 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.

'Sensitive Data' means data pertaining to: racial or ethnic origin; religious or similar beliefs; trade union membership; physical or metal health or sexual life; 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:

1. to receive on request details of the processing relating to themselves. This includes any information about themselves including information regarding the source of the data and about the topic of certain “fully automated decisions”,
2. to have any inaccurate data corrected or removed in a timely fashion,
3. in certain circumstances to stop processing likely to cause “substantial damage or substantial distress”,
4. to prevent their data being used for advertising or marketing,
5. 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 Act.

A fee to cover photocopying and postage charges 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:

1. only authorised people can access, alter, disclose or destroy any personal data,
2. members and employees of the Council only act within the scope of their authority,
3. if personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned.

All personal information held by the Parish 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 anymore or is out of date. Except in exceptional circumstances and is agreed by the Council personal data will be kept for no longer than three years.

Parish Council councillors and staff 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.