

Data Protection Policy (under review June 2008)

This policy was formally adopted by Chilton Town Council (the Council) in August 2004, and applies to all employees and those acting on the Council's behalf.

Scope

An essential activity within the Council is the requirement to gather and process information about its staff and people in the community in order to operate effectively. This will be done in accordance with the Data Protection Act 1998 (the Act), and other related government legislation.

The Council – acting as custodians of personal data – recognises its moral duty to ensure that all such data is handled properly and confidentially at all times, irrespective of whether it is held on paper or by electronic means. This covers the whole lifecycle, including:

- The obtaining of personal data;
- The storage and security of personal data;
- The use of personal data;
- The disposal/destruction of personal data

The Council also has a responsibility to ensure that data subjects have appropriate access – upon written request – to detail regarding personal information relating to them.

Actions

By following and maintaining strict safeguards and controls, the Council will:

- A1. Acknowledge the rights of individual to whom personal data relates, and ensure that these rights may be exercised in accordance with the Act;
- A2. Ensure that both the collection and use of personal data is done fairly and lawfully;
- A3. Ensure that personal data will only be obtained and processed for the purposes specified (in their pursuit of the Council's aims and objectives);
- A4. Collect and process personal data on a "need to know" basis, ensuring that such data is fit for the purpose, is not excessive, and is disposed of at a time appropriate to its purpose;
- A5. Ensuring that adequate steps are taken to ensure that data is current and accurate;
- A6. Ensure that for all personal data, appropriate security measures are taken – both technically and organisationally – to protect against damage, loss or abuse;
- A7. Ensure that the movement of personal data is done in a lawful way – both inside and outside the Council and that suitable safeguards exist at all times.

Enablers

In order to support these actions, the Council will:

- E1. Nominate a **“Data Protection Officer”** for the Council, responsible for gathering and disseminating information and issues relating to information security, the Data Protection Act and other related legislation;
- E2. Ensure that **Chief Officers** are responsible – for communications and issues relating to information security, the Data Protection Act, and other related legislation within their department;
- E3. Ensure that **all activities** that relate to processing ¹of personal data **have appropriate safeguards and controls** in place to ensure information security and compliance with the Act;
- E4. Ensure that all **contracts and service level agreements** (SLAs) between the Council and external third parties – where personal data is processed – **make reference to the Act** as appropriate;
- E5. Ensure that all **staff** acting on the Council’s behalf understand their responsibilities regarding information security under the Act, and that they **receive the appropriate training/instruction and supervision** so that they carry these duties out effectively and consistently and are **given access** to personal information **that is appropriate** to the duties they undertake;
- E6. Ensure that **all third parties** acting on the Council’s behalf **are given access** to personal information **that is appropriate** to the duties they undertake **and no more**;
- E7. Ensure that any requests for **access to personal data are handled courteously, promptly and appropriately**, ensuring that either the data subject or his/her authorised representative has a legitimate right to access under the Act, that the request is valid, and that information provided is clear and unambiguous²;
- E8. Work towards **adopting, as best working practice, the key principles of BS7799** – the British Standard on Information Security Management;
- E9. **Review this policy** and the safeguards and controls that relate to it annually – to ensure that they are still relevant, efficient and effective.

¹ Processing as defined by the Act as obtaining, recording, holding, organisation, adaptation, alteration, retrieval, consultation, use disclosure, alignment, combination, blocking, erasure and destruction.

² All actions regarding data subject access requests will be logged. This audit trail will include details regarding the nature of the request, the steps taken to validate it, the information provided as well as any withheld, e.g. for legal reasons.