Alnwick Town Council
Data Protection Policy (August 2015)

1. Introduction

1.1 An essential activity within the Council is the requirement to gather and process information about its employees 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.

1.2 The Data Protection Act 1998 regulates the way in which certain information about employees and citizens is held and used. Alnwick Town Council considers that many of the principles in the Act represent good practice.

1.3 The implementation and enforcement of this policy in association with the terms and conditions of employment is intended to protect the employee, colleagues, members of the public and the Council.

1.4 This policy bas been formally adopted by Alnwick Town Council and applies to all employees, and those acting on the Council's behalf.

2. Employee Information

2.1 Alnwick Town Council will need to keep information for purposes connected with an employee's employment, including recruitment and termination information. This information will be kept throughout the period of employment and for as long as is necessary following the termination of employment.

2.2 These records may include:

- Information gathered about an employee and any references obtained during recruitment
- Details of terms of employment
- Payroll, tax and National Insurance information
- Performance information
- Details of grade and job duties
- Health records
- Absence records, including holiday records and self certification forms
- Details of any disciplinary investigations and proceedings
- Training records
- Contact names and addresses
- Correspondence with the organisation and other information provided to the organisation.

2.3 The Council believes these uses are consistent with our employment relationship and with the principles of the Act.

2.4 Any information held within the Council is kept in the strictest confidence. In addition, the Council operates a Confidential Reporting Policy which supports our aim that no employee should feel reluctant, for fear of management's response, to give information about any wrongdoing within the organisation.

3. Aims and Scope of this Policy

3.1 This policy is intended to:

- Ensure everyone is aware of their responsibility regarding the Data Protection Act 1998.
- Sets out the basic guidelines for employees.
- Provide a list of definitions to assist in the understanding of the Act.
- Provide information on the types of employee information held by the Council.

4. Guidelines and Principles

4.1 Non adherence or disregard to any of the points below will be seen as a breach of this policy and the disciplinary procedure will be invoked which could result in your dismissal.

4.2 To ensure compliance with the Data Protection Act 1998, the Council will:

1. Acknowledge the rights of individuals to whom personal data relates, and ensure that these rights may be exercised in accordance with the Act;

2. Ensure that both the collection and use of personal data is done fairly and lawfully;

3. Ensure that personal data will only be obtained and processed for the purposes specified;

4. 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;

5. Ensure that adequate steps are taken to ensure the accuracy and currency of data;

6. Ensure that for all personal data, appropriate security measures are taken, both technically and organisationally, to protect against damage, loss or abuse;

7. Ensure that the movement of personal data is done in a lawful way, both inside and outside the Council and those suitable safeguards exist at all times.

8. 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.

9. Treat all employee data with respect and will not obtain or disclose unauthorised, inappropriate or excessive information about individuals.

10. Respond to any information requests under the Data Protection Act within the 40 calendar day time frame.

11. Provide details of exemptions if they apply to a specific request.

12. Destroy or amend inaccurate information when it is brought to light.

13. Charge an administration fee of £10 for each request under the Data Protection Act 1998.

Responsibilities

5 All Staff

5.1 The Council requires all employees to comply with the Data Protection Act in relation to the information about other employees.

5.2 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.

6. The Town Clerk

6.1 The Town Clerk ensures that any third party processing such information on behalf of Alnwick Town Council is contractually obliged to put in place similar measures.

7. Councillors

7.1 Councillors are bound by this policy and must adhere to the guidelines.

8. Freedom of Information

8.1 Under the Freedom of Information Act 2000, the Town Clerk has the responsibility to ensure that data subjects have appropriate access, upon written request, to details regarding personal information relating to them.

9. Data Protection

9.1 The Town Clerk is responsible for gathering and disseminating information and issues relating to information security, the Data Protection Act and other related legislation and ensuring that all staff comply with the legislation.

10. Information Security Policy

10.1 Physical Security

1. Adequate and practical access controls will be provided in all areas where personal and business data is stored or used. Unattended rooms will be secured at all times and doors locked as a minimum security requirement.

2. All documents disclosing identifiable information will be sealed envelopes.

3. Within their level of authority, staff will be responsible for minimising the risk of theft or vandalism of the data and equipment through common-sense precautions. In particular high value equipment such as, laptop computers, will not be left unattended or unsecured and paper records will not be left in public view. All confidential and official information is kept in locked fire proof safes.

4. The physical environment in which data and equipment is stored will be suitable and fit for purpose to ensure the safety of the data and equipment e.g. adequate ventilation for computers, appropriate fire precautions where paper records are stored, controlled access doors. All unattended buildings are alarmed and access is limited via fob or entry code.

10.2 Logical Security

All computerised information and systems are regularly backed up to a secure environment within a fire proof safe.

All computerised information systems will be password controlled.
All passwords will be treated with the strictest confidence and users will not divulge their password to any unauthorised person.

Definitions

11. Personal Data

11.1 Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, telephone number and ID number. It also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

12. Sensitive Data

12.1 Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data are subject to much stricter conditions of processing.

13. Data Controller

13.1 Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

14. Data Subject

14.1 Any living individual who is the subject of personal data held by an organisation.

15. Processing

15.1 Any operation related to organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data, accessing, altering, adding to, merging, and deleting data, retrieval, consultation or use of data, disclosure or otherwise

making available of data.

16. Third Party

16.1 Any individual/organisation other than the data subject, the data controller or its agents.

17. Relevant Filing System

17.1 Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic, CCTV etc. from which the individual's information can be readily extracted.