Data Protection Policy

A guide to the Council's implementation of the Principles set out in the Data Protection Act 1988.

September 2015

Contents Page

Data Protection Policy

1. Introduction

In order to carry out its duties Colchester Borough Council has to collect and use information about the people with whom it works; members of the public; current, past and prospective employees; customers; suppliers and others. In addition the Council often has to collect and use information in order to comply with the requirements of central government.

Colchester Borough Council will ensure that it treats lawfully and correctly all personal information entrusted to it.

2. Statement of Policy

The Council fully endorses and adheres to the Principles set out in the Data Protection Act 1998. ('the Act'). The Council will therefore ensure that all employees, elected members, contractors, agents, consultants, partners or anyone else who has access to any personal data held by or for the Council are fully aware of and abide by their duties and responsibilities under the Act.

This Policy and the procedures set down in it are reviewed annually to ensure that the Council continues to comply with all relevant statutory requirements.

The Council will ensure that all personal data is handled properly and confidentially at all times, irrespective of whether it is held on paper or by electronic means.

This includes:

- the obtaining of personal data;
- the storage and security of personal data;
- the use of personal data;
- the disposal of or destruction of personal data.

The Council will ensure that data subjects have appropriate access, upon written request, to personal information relating to them and the right to correct, rectify, block or erase any incorrect data.

3. The Principles of Data Protection

Whenever collecting or handling information about people the Council will:

1. Ensure that personal data is collected and used fairly and lawfully;

2. Ensure that the purposes for which personal data is obtained and processed are specified and that data is not used for any other purpose;

3. Collect, process and retain personal data only when necessary;

4. Ensure that any data used or kept is accurate and up to date;

5. Ensure that data is disposed of properly as soon as it is no longer needed for the purpose specified when it was collected;

6. Ensure that all personal data is processed in accordance with the rights of the individual concerned

7. Ensure that appropriate security measures are taken to protect all personal data against damage, loss or abuse;

8. 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.

4. Definition of Personal and Sensitive Information

The Act makes a distinction between 'personal data' and 'sensitive personal data':

Personal data is defined as data relating to a living individual who can be identified from that data, or from that data *and* other information which is in the possession of, or is likely to come into the possession of, the data controller. This will include 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.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

5. Roles and Responsibilities

Colchester Borough Council will ensure that:

- A member of staff is appointed who has specific responsibility for data protection within the Council;
- Any disclosure of personal data is in compliance with the law and with approved procedures;
- Anyone managing and handling personal information understands that they are legally bound to follow good data protection practice;

- Anyone managing and handling personal information is appropriately trained and supervised;
- Appropriate advice and guidance is available to anyone wanting to make enquiries about personal information held by the Council;
- Enquiries and requests regarding personal information are handled courteously and within the time limits set by the Act;
- All elected members are to be made fully aware of this policy and of their duties and responsibilities under the Act;
- Where it is necessary to share data that this is done under a written agreement setting out what is to be shared and how it is to be kept secure.

All managers and staff will ensure that:

- Paper files and other records or documents containing personal and or sensitive data are kept securely;
- Personal data held electronically is protected by the use of secure passwords which are changed regularly;
- All users must choose passwords which meet the security criteria specified by the Council;
- Staff working remotely from home or elsewhere must keep any Council owned equipment they use secure and prevent systems and data for which the Council is responsible being used or seen by members of their family or any other unauthorised person.

All contractors, consultants, partners or other servants or agents of the Council must:

- Confirm in writing that they will abide by the requirements of the Act with regard to information obtained from the Council;
- When requested allow the Council data to audit the protection of data held on its behalf;
- Ensure that they and all persons appointed by them who have access to personal data held or processed for or on behalf of the Council are aware of this Policy and are fully trained in their duties and responsibilities under the Act;
- Indemnify the Council without limitation against any prosecutions, claims, proceedings, actions or payments of compensation or damages arising from the loss or misuse of data. Any breach of any provision of the Act will be deemed as being a breach of any contract between the Council and that individual, company, partner or firm.

The Council's Head of Security, supported by the Data Protection Officer, is responsible for:

- Ensuring the provision of cascade data protection training, for staff within the Council.
- The development of best practice guidelines.

- Ensuring compliance checks are undertaken to ensure adherence, throughout the authority, with the Data Protection Act.
- For conducting an annual review of this Data Protection Policy and the practices and procedures pertaining to it to ensure continuing compliance with all relevant statutory provisions.

An officer has also been designated in each service as responsible for ensuring that this Policy is adhered to.

The Council's Chief Executive Officer is the Accountable Officer ultimately responsible for ensuring that all information is appropriately protected.

6. The Information Commissioner

Colchester Borough Council is registered with The Information Commissioner as a data controller.

The Act requires every data controller who is processing personal data to notify and renew their notification on an annual basis. Failure to do so is a criminal offence. Any changes to the type of data held or the purposes for which it is held must be notified to the Information Commissioner, within 28 days.

Designated officers will be responsible for notifying and updating the Data Protection Officer with regard to the processing of personal data within their department.

The Data Protection Officer will review the Data Protection Register with designated officers annually prior to notification to the Information Commissioner.

Disclaimer:

A printed version may not be the current version.

A current version may be obtained in the required format from Colchester Borough Council's Corporate ICT team.