Colchester

Data Protection Policy 2018/19

A statement of the Council's implementation of the principles set out in the Data Protection Act 2018

October 2018

Contents

Data Protection Policy 2018/19

1. CONTEXT

1.1 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.

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

2. APPLICATION OF POLICY

2.1 The Council fully endorses and adheres to the principles set out in the Data Protection legislation (Data Protection Act 2018 and General Data Protection Regulations). 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 data protection legislation.

2.2 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.

2.3 The Council will ensure that all personal data is handled properly and with 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 and processing of personal data;
- the disposal of or destruction of personal data.

2.4 The Council will ensure that data subjects have appropriate access, upon written request, to personal information relating to them and will ensure the data subjects rights to rectification, erasure, restriction, portability and object are adhered to.

3. THE PRINCIPLES OF DATA PROTECTION

3.1 Whenever collecting or handling information about people the Council will:

- Ensure that personal data is processed, lawfully, fairly and in a transparent manner;
- Ensure that the purposes for which personal data is obtained and processed are specified and that data is not used for any other purpose;
- Ensure that processing of personal data is adequate relevant and limited to what is necessary;
- Ensure that any data used or kept is accurate and up to date;
- Ensure that personal data is retained only for as long as necessary;
- Ensure that data is disposed of properly;
- Ensure that all personal data is processed in accordance with the rights of the individual concerned;
- Ensure that personal data is processed in an appropriate manner to maintain security;
- 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 DATA

4.1 The legislation makes a distinction between 'personal data' and 'personal sensitive data':

4.2 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.

4.3 Personal sensitive 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 or sexual orientation;
- Criminal proceedings or convictions;
- Philosophical;
- Genetic data;
- Biometric data.

5. ROLES AND RESPONSIBILITIES

5.1 Colchester Borough Council will ensure that:

- A member of staff, the Data Protection Officer (DPO), 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;
- Members of staff have access only to personal information relevant to their roles;
- 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 out in law;
- All councillors are to be made fully aware of this policy and of their duties and responsibilities under legislation;
- Where personal data may need to be shared with third parties in order to deliver services or perform our duties, the Council will only share personal data when a lawful basis from the legislation can justify that sharing, where it is necessary to achieve a clear purpose and, with that purpose in mind, it is fair and proportionate to do so;
- Data Protection Impact Assessments (DPIA) are conducted, and signed off by the Data Protection Officer and the Senior Information Risk Owner (SIRO) where processing presents a high risk to the privacy of data subjects;
- A record of personal data processing is kept and maintained, this will include a data classification.

5.2 All managers and staff will ensure that:

- Paper files and other records or documents containing personal and or sensitive data are kept securely and destroyed 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;
- Ensure that no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
- Ensure that personal data is not be left where it can be accessed by persons not authorised to see it;

- Take measures to ensure that personal data is kept up to date and accurate;
- Ensure that all personal data is kept in accordance with the Council's retention schedule;
- Ensure that any data protection breaches are swiftly brought to the attention of the Data Protection Officer and that they support the Data Protection Officer assistance in resolving breaches;
- Where there is uncertainty around a data protection matter advice is sought from the Data Protection Officer.

5.3 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 legislation with regard to information obtained from the Council;
- Provide assurance relating to their compliant handling of personal data and when requested allow the Council 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 data protection legislation;
- Ensure that the Council receives prior notification of any disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor;
- 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 DPA 2018 or GDPR will be deemed as being a breach of any contract between the Council and that individual, company, partner or firm.

5.4 The Council's Data Protection Officer, is responsible for:

- Advising the Council and its staff of its obligations under data protection legislation;
- 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 Data Protection legislation;
- Providing advice where requested on data protection impact assessments;
- To co-operate with and act as the contact point for the Information Commissioner's Office;
- 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.

5.5 The Councils Senior Information Risk Owner, is responsible for:

- Being the organisations leader and Champion for Information Risk Management and Assurance;
- Advocating good information management and security practices;
- Acting in an arbitrary role – to challenge risk mitigation;
- Ensuring others are undertaking risk assessments and assurance activities;
- Reporting annually to the Accountable Officer;
- Being the senior manager with accountability for data protection and information risk and provides a link to the Council's senior management team (SMT).

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

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

6. COUNCILLORS

6.1 This policy applies to councillors, and all councillors are made aware of the advice produced by the Information Commissioners Office, which can be read by clicking on the link below:

https://ico.org.uk/media/for-organisations/documents/1432067/advice-for-elected-and-prospective-councillors.pdf

6.2 Councillors must be registered with the Information Commissioner as data controllers.

7. THE INFORMATION COMMISSIONER

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

7.2 The Data Protection Act 2018 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.

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

7.4 The Data Protection Officer will review the Information Asset Register with designated officers annually.

FURTHER INFORMATION

Contact

ICT

ICT@colchester.gov.uk

Data Protection Officer

DPO@colchester.gov.uk

01206 507340

In the event of an information breach, or suspected breach, contact the ICT team and the Data Protection Officer.