# Data Protection Policy

August 2021

Customer Business Culture

# Data Protection Policy

## CONTEXT

Colchester Borough Council needs 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 order to carry out its duties. This Data Protection Policy sets out the organisation's commitment and approach to data protection and provides a clear frame of reference for employees to determine the organisation's standards, aims, and ideals in respect of data protection compliance.

The processing of personal data in the United Kingdom is regulated by law. The principle statutory instrument setting out the legal obligations of those handling personal data is the Data Protection Act 2018 (DPA 2018). Other laws inter-relate with the DPA 2018 including, but not limited to, the General Data Protection Regulation (GDPR), the Privacy and Electronic Communications Regulations (2003) and the Freedom of Information Act (2000). These laws are collectively referred to in this Policy as Data Protection Legislation.

## POLICY STATEMENT

Colchester Borough Council is committed to compliance with all relevant Data Protection Legislation and will formally delegate appropriate powers and responsibilities to its personnel to ensure that it is fully able to comply with Data Protection Legislation and its own defined standards in the field of data protection and information governance.

The Council will ensure that sufficient and appropriate resources are available to ensure that it meets both its legal obligations in respect of Data Protection Legislation and the standards that it sets through its policies. The Council will ensure that the organisation works within the 6 data protection principles and that it will implement sufficient controls to ensure that it is able to demonstrate compliance with the Data Protection Legislation including the keeping of sufficient records of data processing activities, risk assessments and decisions relating to data processing activities.

The Council will uphold the rights and freedoms of people conferred on them by the Data Protection Legislation. It will ensure that those rights and freedoms are appropriately taken into account in the decisions it takes which may affect people and will ensure that it has sufficient controls in place to assist people who wish to exercise their rights. 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.

This policy applies to all Council activities and operations which involve the processing of personal data. This policy applies to anyone who is engaged to process personal data for or on behalf of the Council including: employees, volunteers, casual and temporary staff, directors and officers, Councillors and third-parties such as sub-contractors and suppliers, and anyone who the Council shares or discloses personal data with/to.

The Council will ensure that all personal data is handled properly and with confidentiality, 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.

## THE PRINCIPLES OF DATA PROTECTION

Whenever collecting or handling information about people the Council will ensure that:

- Personal data is processed, lawfully, fairly and in a transparent manner
    - No data collection activities will be undertaken or commissioned without an appropriate privacy notice being provided to the person about whom data are being collected
    - No data collection activities will be undertaken or commissioned without there being a lawful ground for the data processing activities intended to be applied to the personal data
- The purposes for which personal data is obtained and processed are specified and that data is not used for any other purpose
- Processing of personal data is adequate relevant and limited to what is necessary
- It uses reasonable endeavours to maintain data as accurate and up-to-date as possible
- Personal data is retained only for as long as necessary
    - The Council will maintain a data retention schedule setting out approved retention periods
- Data is disposed of properly
- All personal data is processed in accordance with the rights of the individual concerned
- Personal data is processed in an appropriate manner to maintain security
- 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.
- A Data Breach Reporting Procedure is maintained
    - All employees and those with access to personal data are aware of it
    - The Council will log all personal data breaches and will investigate each incident without delay
    - Appropriate remedial action will be taken as soon as possible to isolate and contain the breach, evaluate and minimise its impact, and to recover from the effects of the breach
- Periodic compliance checks are completed to test whether its policies and procedures are being adhered to and to test the effectiveness of control measures
- They strive to foster a culture of data protection by design and by default in all data processing activities

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

## DEFINITION OF SPECIAL CATEGORY DATA

The legislation makes a distinction between 'personal data' and 'special category 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.

Special category 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.

## ROLES AND RESPONSIBILITIES

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
- 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 staff and councillors are fully aware of this policy and of their duties and responsibilities under Data Protection 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.

Everyone will ensure that:

- All data processing operations under their control or sphere of responsibility or commissioned by them are undertaken in compliance with this policy and other relevant data protection policies
- Paper files and other records or documents containing personal and or special category data are kept securely and destroyed securely
- Personal data held electronically is protected by the use of secure passwords
- 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
- No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party
- Personal data is not stored on personal devices or forwarded to personal email accounts
- Personal data is not to be left where it can be accessed by persons not authorised to see it
- Personal data is kept up to date and accurate
- Personal data is kept in accordance with the Council's retention schedule
- Any data protection breaches are swiftly brought to the attention of the Data Protection Officer and that they support the Data Protection Officer in resolving breaches
- Where there is uncertainty around a data protection matter advice is sought from the Data Protection Officer.

The Council reserves the right to contract out data processing activities or operations involving the processing of personal data in the interests of business efficiency and effectiveness. No third-party data processors will be appointed who are unable to provide satisfactory assurances that they will handle personal data in accordance with the Data Protection Legislation. All processors, contractors, consultants, partners 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 Data Protection Act 2018 (DPA 2018) or the General Data Protection Regulations (GDPR) will be deemed as being a breach of any contract between the Council and that individual, company, partner or firm.

The Council's Data Protection Officer is responsible for:

- Ensuring that staff are aware of this policy
- 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 (ICO)
- 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.

The Council's Senior Information Risk Owner, is responsible for:

- Ensuring appropriate mechanisms are in place to support service delivery and continuity
- Being the organisation's 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
- Is the senior manager with accountability for data protection and information risk and provides a link to the Council's Senior Management Team (SMT).

## COUNCILLORS

This policy applies to Councillors, and all Councillors are made aware of the advice produced by the Information Commissioners Office (ICO).

## THE INFORMATION COMMISSIONER

Colchester Borough Council is registered with The Information Commissioner as a data controller. The DPA 2018 requires every data controller who is processing personal data to notify and renew their notification on an annual basis.

## POLICY REVIEW

The policy will be reviewed on an annual basis and updated as necessary at these reviews.

## FURTHER INFORMATION

For further information about Colchester Borough Council's compliance with Data Protection Legislation, please visit www.colchester.gov.uk/privacy or email dpo@colchester.gov.uk.

## VERSION CONTROL

| | |
|---|---|
| Purpose: | To specify how the Council complies with Data Protection Legislation |
| Status: | Draft |
| Final date: | |
| To be reviewed: | August 2022 |