

23 November 2021

Report of	Monitoring Officer	Author	Andrew Weavers ☎ 282213
Title	Review of the Council's Ethical Governance Policies		
Wards affected	Not applicable		

1. Executive Summary

- 1.1 This report requests the Committee to review the Council's updated Ethical Governance policies. These are the key policies which set out the standards of conduct and integrity that the Council expects of councillors, staff, partners, suppliers and customers when conducting Council business. They contain procedures for dealing with breaches of the policies and processes to be followed.
- 1.2 The report also requests the Committee to recommend to Full Council to include the updated policies in the Policy Framework which comprises all of the Authority's key policies.

2. Recommended Decision

- 2.1 To recommend to Full Council that it adopts the statement of intent in relation to ethical governance.
- 2.2 To review the following revised policies:
 - Anti-Fraud and Corruption Policy
 - Whistleblowing Policy
 - Anti-Money Laundering Policy
 - Covert Surveillance Policy
 - Colchester Borough Council Social Media RIPA Policy
 - Data Protection Policy
 - Acceptable Use Policy
 - Information Security Policy
 - Retention Policy
 - Income and Debt Management Policy

and to recommend to Full Council that they be approved for inclusion in the Council's Policy Framework.

3. Background

- 3.1 The Council is committed to maintaining the highest standards of governance including the elimination of fraud and corruption and to ensuring that all activities are conducted ethically, honestly, openly and accountably in order to protect public safety and public money.
- 3.2 A varied range of policies and procedures form the Corporate Governance framework and a selection of these relate to Ethical Governance - those specifically regarding conduct and integrity.

- 3.3 The Ethical Governance policies set out the standards of conduct and integrity that it expects from staff, elected members, suppliers, partners, volunteers and the public. Breaches of the policies will be pursued, and procedures have been introduced to enable any person to raise genuine concerns they may have about the conduct of anybody acting for or on behalf of the Council.
- 3.4 At its meeting on 3 December 2020 Full Council adopted a statement of intent in relation to both Ethical and Corporate Governance which gave a high organisational commitment to zero tolerance of fraud, corruption and bribery. It is appropriate following the change of Administration and Leader to refresh the statement of intent which is attached at Appendix 1. The Committee is recommended to refer this to Full Council for adoption.

4. Review of Ethical Governance Policies

- 4.1 The Anti-Fraud and Corruption, Whistleblowing, Anti-Money Laundering, Covert Surveillance, Information Security, Data Protection, Acceptable Use, Data Retention and Income and Debt policies were last reviewed by this Committee at its meeting on 24 November 2020. The Ethical Governance policies were subsequently adopted as part of the Council's Policy Framework by Full Council.

The following table indicates the number of times a policy was invoked in the past year and where appropriate whether it was effective.

Policy	No. of times invoked during 2017/18	No. of times invoked during 2018/19	No. of times invoked during 2019/20	No. of times invoked during 2020/21	Whether procedures effective
Anti-Fraud and Corruption	None	None	None	None	n/a
Whistleblowing	None	1	None	None	n/a
Anti-Money Laundering	None	None	None	None	n/a
Covert Surveillance	None	None	None	None	n/a
Information Security	None	None	None	None	n/a
Data Protection	None	None	None	None	n/a
Acceptable Use	-	-	None	None	n/a
Data Retention	-	-	None	None	n/a

- 4.2 The Anti-Fraud and Corruption, Whistleblowing, Anti-Money Laundering, Covert Surveillance, Information Security, Data Protection, Acceptable Use and Data Retention policies have all been reviewed to ensure that they remain fit for purpose and no changes are proposed to these policies which are appended to this report.
- 4.3 The Committee at its meeting on 7 September 2021 considered and agreed a new Processing of Special Category & Criminal Convictions Personal Data Policy. This was subsequently endorsed by Full Council at its meeting on 20 October 2021 and was included as part of the Council's Policy Framework. This Policy will be reviewed annually going forward as part of the annual review of ethical governance policies.
- 4.4 The Monitoring Officer writes an annually to both Members and Officers reminding them of their obligations regarding the Anti-Fraud and Corruption and Whistleblowing policies. Councillors have recently received updated data protection and cyber security training from the Council's IT team.
- 4.5 The Income & Debt Management Policy has been reviewed and there are no proposed changes for this year. The processes are still relevant and meet legislative requirements, whilst supporting strong collection rates.

- 4.6 During the last full financial year, the Council achieved high collection rates for Council Tax despite the impacts of Covid-19, this has continued into 2021/22. Business rates collection has been more significantly impacted, with those not supported through Government grants or relief still struggling to pay. The Council has worked to support those struggling whilst encouraging flexible arrangements to maintain some payments from those businesses most affected. It is anticipated that the ongoing effects of Covid-19 will impact on business rates collection through to 2022/23.
- 4.7 The Council continues to improve processes, making payment options simple for residents and businesses and encouraging customers to contact as soon as possible if they are suffering financial difficulties.

5. Strategic Plan References

- 5.1 The manner in which the Council governs its business is an underpinning mechanism in the Council's Strategic Plan priorities to set out the direction and future potential for our Borough.

6. Publicity Considerations

- 6.1 The Council's ethical governance policies will be published on the Council's website.

7. Financial, Equality, Diversity and Human Rights, Consultation, Health, Wellbeing and Community Safety, Health and Safety, Risk Management and Environmental and Sustainability Implications

- 7.1 None.

Ethical Governance Statement 2021/22

Colchester Borough Council will not tolerate breaches of its ethical governance policies.

The Council is committed to maintaining the highest standards of governance including the elimination of fraud and corruption and to ensuring that all activities are conducted ethically, honestly, openly and accountably so as to protect public safety and public money.

The Council expects the highest standards of conduct and integrity from all that have dealings with it including staff, elected members, suppliers, partners, volunteers and the public. Therefore, policies have been put in place to outline the standards required and procedures have been introduced to enable any person to raise genuine concerns they may have about the conduct of anybody acting for or on behalf of the Council.

The Ethical Governance policies form part of the Council's overall Corporate Governance framework and details of all the policies have been published on the Council's website at www.colchester.gov.uk.

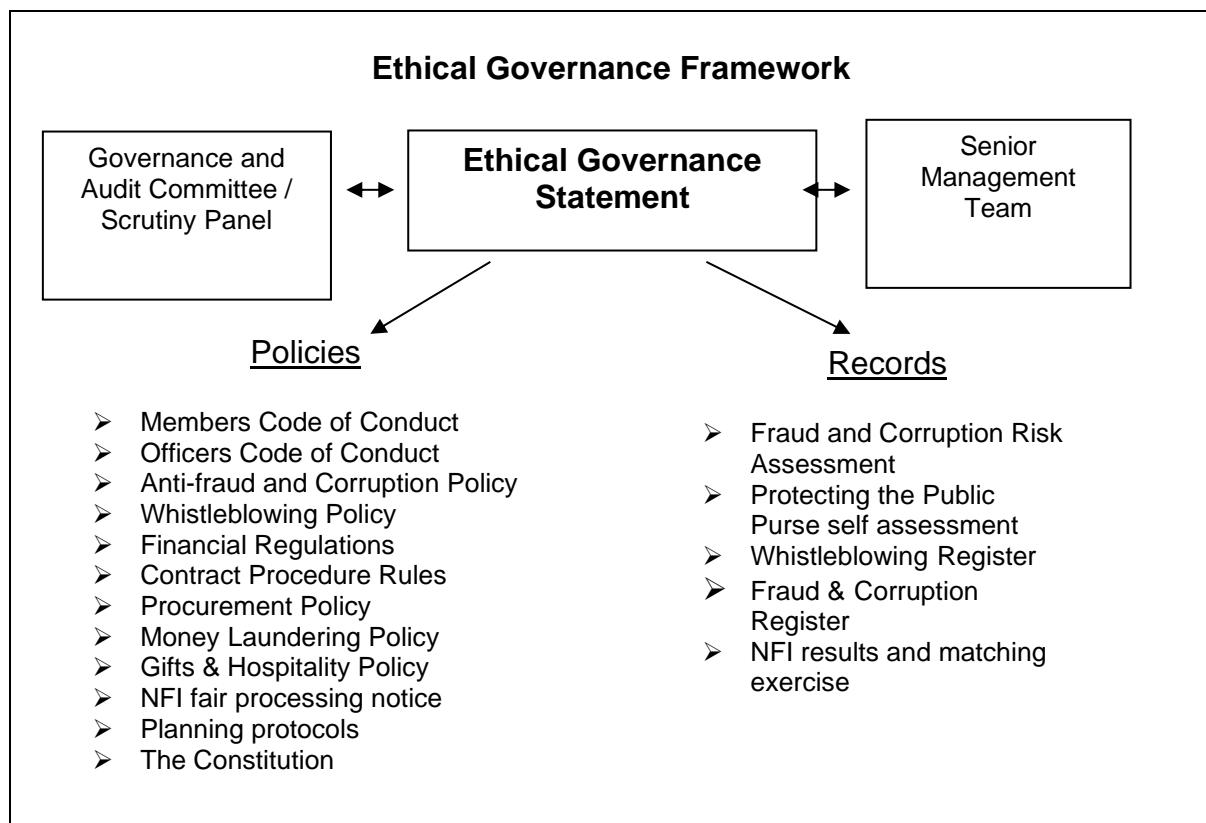
We will take all reasonable steps to ensure that concerns are investigated, and appropriate action taken where necessary. There will be no distinction made in investigation between cases that generate financial benefits and those that do not.



Paul Dundas
Leader of the Council



Adrian Pritchard
Chief Executive





Anti-Fraud and Corruption Policy 2021/22

A guide to the Council's approach to preventing fraud and corruption and managing any suspected cases

November 2021

Contents

Page

1.0	INTRODUCTION	1
2.0	OVERVIEW	1
3.0	CULTURE	2
4.0	RESPONSIBILITIES AND PREVENTION	3
4.1	Responsibilities of Elected Members	3
4.2	Responsibilities of the Monitoring Officer	3
4.3	Responsibilities of the Section 151 Officer	3
4.4	Responsibilities of the Senior Management Team	4
4.5	Responsibilities of Employees	4
4.6	Role of Internal Audit	4
4.7	Role of the Benefits Investigation	5
4.8	Role of the Corporate Governance Team	5
4.9	Role of the External Auditors	5
4.10	Role of the Public	5
4.11	Conflicts of Interest	5
4.12	Official Guidance	5
5.0	DETECTION AND INVESTIGATION	6
5.1	Disciplinary Action	6
5.2	Prosecution	6
5.3	Publicity	6
6.0	AWARENESS AND MONITORING	7

ANTI-FRAUD AND CORRUPTION POLICY

1.0 INTRODUCTION

Colchester Borough Council, like every Local Authority, has a duty to ensure that it safeguards the public money that it is responsible for.

The Council expects the highest standards of conduct and integrity from all that have dealings with it including staff, members, contractors, volunteers and the public. It is committed to the elimination of fraud and corruption and to ensuring that all activities are conducted ethically, honestly and to the highest possible standard of openness and accountability so as to protect public safety and public money.

All suspicions or concerns of fraudulent or corrupt practise will be investigated. There will be no distinction made in investigation and action between cases that generate financial benefits and those that do not. Any investigations will not compromise the Council's commitment to Equal Opportunities or the requirements of the Human Rights Act or any other relevant statutory provision.

This policy has been created with due regard to the CIPFA better Governance Forum's Red Book 2 'Managing the Risk of Fraud', the CIPFA 2014 Code of Practice on Managing the Risk of Fraud and Corruption and the Audit Commission publication 'Protecting the Public Purse'.

2.0 OVERVIEW

This policy provides an overview of the measures designed to combat any attempted fraudulent or corrupt act. For ease of understanding it is separated into four areas as below:

- Culture
- Responsibilities and Prevention
- Detection and Investigation
- Awareness and Monitoring.

Fraud and corruption are defined as:

Fraud – “the intentional distortion of financial statements or other records by persons internal or external to the Council, which is carried out to conceal the misappropriation of assets or otherwise for gain”.

In addition, fraud can also be defined as “the intentional distortion of financial statements or other records by persons internal or external to the authority, which is carried out to mislead or misrepresent”.

Corruption – “the offering, giving, soliciting or acceptance of an inducement or reward which may influence the action of any person”.

The Council also abides by the Bribery Act 2010 which covers, amongst other things, the offences of bribing another person, of allowing to be bribed and organisational responsibility. Such offences include:

- The offer, promise or giving of financial or other advantage to another person in return for the person improperly performing a relevant function or activity
- Requesting, agreeing to receive or accepting a financial or other advantage intending that, in consequence a relevant function or activity should be performed improperly.
- Commercial organisation responsibility for a person, associated with the organisation, bribing another person for the purpose of obtaining or retaining business for the organisation.

In addition, this policy also covers “the failure to disclose an interest in order to gain financial or other pecuniary benefit.”

3.0 CULTURE

The prevention/detection of fraud/corruption and the protection of public money are responsibilities of everyone, both internal and external to the organisation. The Council's elected members and employees play an important role in creating and maintaining this culture. They are positively encouraged to raise concerns regarding fraud and corruption, immaterial of seniority, rank or status, in the knowledge that such concerns will, wherever possible, be treated in confidence. The public also has a role to play in this process and should inform the Council if they feel that fraud/corruption may have occurred.

Concerns must be raised when members, employees or the public reasonably believe that one or more of the following has occurred, is in the process of occurring or is likely to occur:

- A criminal offence
- A failure to comply with a statutory or legal obligation
- Improper or unauthorised use of public or other official funds
- A miscarriage of justice
- Maladministration, misconduct or malpractice
- Endangering an individual's health and/or safety
- Damage to the environment
- Deliberate concealment of any of the above.

The Council will ensure that any allegations received in any way, including by anonymous letter or telephone call, will be taken seriously and investigated in an appropriate manner. The Council has a whistle blowing policy that sets out the approach to these types of allegations in more detail.

The Council will deal firmly with those who defraud the Council or who are corrupt, or where there has been financial malpractice. There is, of course, a need to ensure that any investigation process is not misused and, therefore, any abuse (such as employees/members raising malicious allegations) may be dealt with as a disciplinary matter (employees) or through Group procedures (Members).

When fraud or corruption has occurred due to a breakdown in the Council's systems or procedures, Directors will ensure that appropriate improvements in systems of control are implemented in order to prevent a re-occurrence.

4.0 RESPONSIBILITIES AND PREVENTION

4.1 Responsibilities of Elected Members

As elected representatives, all members of the Council have a duty to protect the Council and public money from any acts of fraud and corruption. This is done through existing practice, compliance with the Council's Members' Code of Conduct, the Council's Constitution including Financial Regulations and Standing Orders and relevant legislation. Conduct and ethical matters are specifically brought to the attention of members during induction and include the declaration and registration of interests. Officers advise members of new legislative or procedural requirements.

4.2 Responsibilities of the Monitoring Officer

The Monitoring Officer is responsible for ensuring that all decisions made by the Council are within the law. The Monitoring Officer's key role is to promote and maintain high standards of conduct throughout the Council by developing, enforcing and reporting appropriate governance arrangements including codes of conduct and other standards policies.

All suspected instances of fraud or corruption (apart from benefit claim issues) should be reported to the Monitoring Officer.

4.3 Responsibilities of the Section 151 Officer

The Head of Finance has been designated with the statutory responsibilities of the Finance Director as defined by s151 of the Local Government Act 1972. These responsibilities outline that every local authority in England and Wales should: "make arrangements for the proper administration of their financial affairs and shall secure that one of their officers has the responsibility or the administration of those affairs"

'Proper administration' encompasses all aspects of local authority financial management including:

- Compliance with the statutory requirements for accounting and internal audit;
- Managing the financial affairs of the Council
- The proper exercise of a wide range of delegated powers both formal and informal;
- The recognition of the fiduciary responsibility owed to local tax payers.

Under these statutory responsibilities the Section 151 Officer contributes to the anti-fraud and corruption framework of the Council.

4.4 Responsibilities of the Senior Management Team

Managers at all levels are responsible for the communication and implementation of this policy. They are also responsible for ensuring that their employees are aware of the Council's personnel policies and procedures, the Council's Financial Regulations and Standing Orders and that the requirements of each are being met. Managers are expected to create an environment in which their staff feel able to approach them with any concerns they may have about suspected irregularities. Special arrangements may be applied from time to time for example where employees are responsible for cash handling or are in charge of financial systems and systems that generate payments, for example payroll or the Revenues and Benefits computer system. These procedures will be supported by relevant training.

The Council recognises that a key preventative measure in dealing with fraud and corruption is for managers to take effective steps at the recruitment stage to establish, as far as possible, the honesty and integrity of potential employees, whether for permanent, temporary or casual posts and agency staff. The Council's formal recruitment procedure contains appropriate safeguards in the form of written references, the verification of qualifications held and employment history. Disclosure and Barring Service (DBS) checks are undertaken for employees working with or who may have contact with children or vulnerable adults.

4.5 Responsibilities of Employees

Each employee is governed in their work by the Council's Standing Orders and Financial Regulations, and other policies on conduct and IT usage. Included in the Council policies are guidelines on Gifts and Hospitality, and codes of conduct associated with professional and personal conduct and conflict of interest. These are issued to all employees when they join the Council. In addition, employees are responsible for ensuring that they follow any instructions given to them, particularly in relation to the safekeeping of the assets of the Council. Employees are expected always to be aware of the possibility that fraud, corruption and theft may exist in the workplace and be able to share their concerns with management.

4.6 Role of Internal Audit

Internal Audit plays a preventative role in trying to ensure that systems and procedures are in place to prevent and deter fraud and corruption. Internal Audit may be requested to investigate cases of suspected financial irregularity, fraud or corruption, except Benefit Fraud investigations, in accordance with agreed procedures. Within the Financial Regulations in the Constitution, representatives of Internal Audit are empowered to:

- enter at all reasonable times any Council premises or land
- have access to all records, documentation and correspondence relating to any financial and other transactions as considered necessary
- have access to records belonging to third parties such as contractors when required
- require and receive such explanations as are regarded necessary concerning any matter under examination

- require any employee of the Council to account for cash, stores or any other Council property under their control or possession
Internal Audit liaises with management to recommend changes in procedures to reduce risks and prevent losses to the Authority.

4.7 Role of the Benefits Investigation

Any allegations of benefit fraud are to be referred to the Department of Work and Pensions for investigation.

4.8 Role of the Corporate Governance Team

The team consists of various officers whose roles include governance issues and the objective is to promote and embed a governance culture throughout the organisation by implementing policies, reviewing issues, providing training and sharing information.

4.9 Role of the External Auditors

Independent external audit is an essential safeguard of the stewardship of public money. This is currently carried out by BDO UK LLP through specific reviews that are designed to test (amongst other things) the adequacy of the Council's financial systems and arrangements for preventing and detecting fraud and corruption. It is not the external auditors' function to prevent fraud and irregularities, but the integrity of public funds is at all times a matter of general concern. External auditors are always alert to the possibility of fraud and irregularity and will act without undue delay if grounds for suspicion come to their notice. The Council contributes to the bi-annual National Fraud Initiative which is designed to cross-match customers across authorities to highlight areas where there are potential fraudulent claims.

4.10 Role of the Public

This policy, although primarily aimed at those within or associated with the Council, enables concerns raised by the public to be investigated, as appropriate, by the relevant person in a proper manner.

4.11 Conflicts of Interest

Both elected members and employees must ensure that they avoid situations where there is a potential for a conflict of interest. Such situations can arise with externalisation of services, internal tendering, planning and land issues etc. Effective role separation will ensure decisions made are seen to be based upon impartial advice and avoid questions about improper disclosure of confidential information.

4.12 Official Guidance

In addition to Financial Regulations and Standing Orders, due regard will be had to external and inspectorate recommendations.

The Council is aware of the high degree of external scrutiny of its affairs by a variety of bodies such as Government Inspection bodies, the Local Government and Social Care Ombudsman, HM Customs and Excise and the Inland Revenue. These bodies are important in highlighting any areas where improvements can be made.

5.0 DETECTION AND INVESTIGATION

Internal Audit plays an important role in the detection of fraud and corruption. Included within the audit plans are reviews of system controls including financial controls and specific fraud and corruption tests, spot checks and unannounced visits.

In addition to Internal Audit, there are numerous systems and management controls in place to deter fraud and corruption, but it is often the vigilance of employees and members of the public that aids detection. In some cases, frauds are discovered by chance or “tip-off” and the Council will ensure that such information is properly dealt with within its whistleblowing policy.

Detailed guidance on the investigation process is available separately.

5.1 Disciplinary Action

The Council’s Disciplinary Procedures will be used to facilitate a thorough investigation of any allegations of improper behaviour by employees. Theft, fraud and corruption are serious offences which may constitute gross misconduct against the Council and employees will face disciplinary action if there is evidence that they have been involved in these activities, including Benefit fraud. Disciplinary action will be taken in addition to, or instead of, criminal proceedings depending on the circumstances of each individual case.

Members will face appropriate action under this policy if they are found to have been involved in theft, fraud and corruption against the Council. Action will be taken in addition to, or instead of criminal proceedings, depending on the circumstances of each individual case but in a consistent manner. If the matter is a breach of the Members’ Code of Conduct, then it will be dealt with in accordance with the Arrangements agreed by the Council in accordance with the Localism Act 2011.

5.2 Prosecution

In terms of proceedings the Council will endeavour to take action in relevant cases to deter others from committing offences against the Council.

5.3 Publicity

The Council will optimise the publicity opportunities associated with anti-fraud and corruption activity within the Council. Wherever possible, where the Council has suffered a financial loss action will be taken to pursue the recovery of the loss. All anti-fraud and corruption activities, including the update of this policy, will be publicised.

6.0 AWARENESS AND MONITORING

The Council recognises that the continuing success of this policy and its general credibility will depend in part on the effectiveness of training and awareness for members and employees and will therefore take appropriate action to raise awareness levels.

The Monitoring Officer will provide an annual report to senior management and members outlining investigations undertaken during the year.

This policy and associated procedures will be reviewed at least annually and will be reported to senior management and the Governance and Audit Committee.



Whistleblowing Policy

2021/22

A guide for employees and Councillors
on how to raise concerns about conduct
within the Council

November 2021

Contents	Page
1.0 Introduction	1
2.0 Aims and Scope of the Whistleblowing Policy	1
3.0 Safeguards	2
3.1 Harassment or Victimisation	2
3.2 Confidentiality	3
3.3 Anonymous Allegations	3
3.4 Untrue Allegations	3
4.0 How to raise a concern	3
5.0 How the Council will respond	4
6.0 The Responsible Officer	5
7.0 How the matter can be taken further	5
8.0 Questions regarding this policy	6
9.0 Review	6

WHISTLEBLOWING POLICY

1.0 Introduction

Employees or Councillors are often the first to realise that there may be some form of inappropriate conduct within the Council. However, they may not express their concerns because they feel that speaking up would be disloyal to their colleagues or to the Council. They may also fear harassment or victimisation. In these circumstances it may be easier to ignore the concern rather than report what may just be a suspicion of misconduct, but this can have serious consequences if wrongdoing goes undetected.

The Council is committed to the highest possible standards of openness, probity, accountability and honesty. In line with that commitment we expect employees, councillors and others that we deal with who have serious concerns, about any aspect of the Council's work, to come forward and voice those concerns.

This policy document makes it clear that employees and councillors can do so without fear of victimisation, subsequent discrimination or disadvantage. This Whistleblowing Policy and Procedure is intended to encourage and enable employees and councillors to raise serious concerns within the Council rather than overlooking a problem or 'blowing the whistle' outside. With the exception of employment related grievances, this policy will apply to any act of Whistleblowing, as defined by the charity Public Concern at Work to mean; "A disclosure of confidential information which relates to some danger, fraud or other illegal or unethical conduct connected with the workplace, be it of the employer or of its employees."

This policy and procedure applies to all employees, councillors, partners, volunteers and contractors. It also covers suppliers and members of the public.

These procedures are in addition to the Council's complaints procedures and other statutory reporting procedures. Officers are responsible for making customers aware of the existence of these procedures.

This policy has been discussed with the relevant trade unions and has their support.

2.0 Aims and Scope of the Whistleblowing Policy

This policy aims to:

- Encourage you to feel confident in raising serious concerns and to question and act upon concerns about practice without fear of recrimination.
- Provide avenues for you to raise those concerns and receive feedback on any action taken.
- Ensure that you receive a response to your concerns and that you are aware of how to pursue them if you are not satisfied.

- Reassure you that you will be protected from possible reprisals or victimisation if you have a reasonable belief that you have made any disclosure in good faith.
- Advise you of the support that the Council will provide if you raise concerns in good faith.

There are existing procedures in place to enable you to lodge a grievance relating to your own employment. This Whistleblowing Policy and Procedure is intended to cover major concerns that fall outside the scope of other procedures. These include:

- conduct which is an offence or a breach of law
- disclosures related to miscarriages of justice
- health and safety risks, including risks to the public as well as other employees
- damages to the environment
- the unauthorised use of public funds
- possible fraud and corruption
- other unethical conduct
- unacceptable business risks.

This concern may be about something that:

- makes you feel uncomfortable in terms of known standards, your experience or the standards you believe the Council subscribes to; or
- is against the Council's Procedure Rules and policies; or
- falls below established standards of practice; or
- amounts to improper conduct.

3.0 Safeguards

3.1 Harassment or Victimisation

The Council is committed to good practice and high standards and wants to be supportive of employees and councillors.

The Council recognises that the decision to report a concern can be a difficult one to make. If what you are saying is true, you should have nothing to fear because you will be doing your duty to the Council and those for whom you are providing a service. In these situations, you are a witness and not a complainant.

The Council will not tolerate the harassment or victimisation of any person who raises a concern. The Council's disciplinary procedures will be used against any employee who is found to be harassing or victimising the person raising the concern and such behaviour by a councillor will be reported under the Members' Code of Conduct.

Any investigation into allegations of potential malpractice will not influence or be influenced by any disciplinary or redundancy procedures that already affect you if you are an employee.

3.2 Confidentiality

All concerns will be treated in confidence and the Council will do its best to protect your identity if you do not want your name to be disclosed. If investigation of a concern discloses a situation that is sufficiently serious to warrant disciplinary action or police involvement, then your evidence may be important. Your name will not however be released as a possible witness until the reason for its disclosure, at this stage, has been fully discussed with you.

3.3 Anonymous Allegations

This policy encourages you to put your name to your allegation whenever possible.

Concerns expressed anonymously are much less powerful but will be considered at the discretion of the Council.

In exercising this discretion, the factors to be taken into account would include the:

- seriousness of the issues raised;
- credibility of the concern; and
- likelihood of confirming the allegation from attributable sources.

3.4 Untrue Allegations

If you make an allegation in good faith, but it is not confirmed by the investigation, no action will be taken against you. If however, you make an allegation maliciously or for personal gain, disciplinary action may be taken against you, or if you are a councillor a complaint may be made under the Members' Code of Conduct.

4.0 How to raise a concern

You should normally raise concerns with the Monitoring Officer or the Section 151 Officer. However, if your concern relates to one of these officers you should raise your concerns with the Chief Executive.

Concerns may be raised verbally or in writing. Employees or councillors who wish to make a written report are invited to use the following format:

- the background and history of the concern (giving relevant dates);
and
- the reason why you are particularly concerned about the situation.

The earlier you express the concern the easier it is to take action.

Although you are not expected to prove beyond doubt the truth of an allegation, you will need to demonstrate to the person contacted that there are reasonable grounds for your concern.

Advice and guidance on how matters of concern may be pursued can be obtained from:

Chief Executive, Adrian Pritchard ☎ 282211

Monitoring Officer, Andrew Weavers ☎ 282213

Section 151 Officer, Paul Cook ☎ 505861

Deputy Monitoring Officer, Hayley McGrath ☎ 508902

Deputy Monitoring Officer, Julian Wilkins ☎ 282257.

You may wish to consider discussing your concern with a colleague first and you may find it easier to raise the matter if there are two (or more) of you who have had the same experience or concerns.

If you are an employee you may invite your trade union or a friend to be present during any meetings or interviews in connection with the concerns you have raised. If you are a councillor you may be accompanied by your group leader.

The Council has a dedicated email address whistleblowing@colchester.gov.uk

Further guidance on protection for anyone raising a concern can be found in the Public Interests Disclosure Act 1998.

5.0 How the Council will respond

The Council will respond to your concerns. Do not forget that testing out your concerns is not the same as rejecting them.

Where appropriate, the matters raised may be:

- investigated by management, Internal Audit, or through the disciplinary process
- referred to the police
- referred to the Council's external auditor
- the subject of an independent inquiry.

In order to protect individuals and those accused of misdeeds or possible malpractice, initial enquiries will be made to decide whether an investigation is appropriate and, if so, what form it should take. The overriding principle, which the Council will have in mind, is the public interest.

Some concerns may be resolved by agreed action without the need for investigation.

Within **five** working days of a concern being raised, one of the named Officers will write to you:

- acknowledging that the concern has been received
- indicating how it is proposed to deal with the matter
- giving an estimate of how long it will take to provide a final response

- informing you whether any initial enquiries have been made
- supplying you with information on staff support mechanisms, and
- informing you whether further investigations will take place and if not, why not.

The amount of contact between the officers considering the issues and you will depend on the nature of the matters raised, the potential difficulties involved, and the clarity of the information provided. If necessary, the Council will seek further information from you.

Where any meeting is arranged, off-site where appropriate, if you so wish, you can be accompanied by a union or professional association representative or a friend, or the group leader if you are a councillor.

The Council will take steps to minimise any difficulties, which you may experience as a result of raising a concern. For instance, if you are required to give evidence in criminal or disciplinary proceedings the Council will arrange for you to receive advice about the procedure and will help you with the preparation of statements.

The Council accepts that you need to be assured that the matter has been properly addressed. Thus, subject to legal constraints, you will receive information about the outcomes of any investigation.

6.0 The Responsible Officer

The Monitoring Officer has overall responsibility for the maintenance and operation of this policy. That officer maintains a record of concerns raised and the outcomes (but in a form which does not endanger your confidentiality) and will provide an annual report on the operation of the policy to the Governance and Audit Committee.

7.0 How the matter can be taken further

This policy is intended to provide you with an avenue to raise concerns within the Council. The Council hopes you will be satisfied with any action taken. If you are not, and if you feel it is right to take the matter outside the Council, the following are possible contact points:

- (a) Citizens Advice Bureau
- (b) relevant professional bodies or regulatory organisations
- (c) the police
- (d) Local Government and Social Care Ombudsman
- (e) the Council's Governance and Audit Committee.

If you are considering taking the matter outside of the Council, you should ensure that you are entitled to do so and that you do not disclose confidential information.

An independent charity, Protect, can offer independent and confidential advice. Protect can be contacted via their advice line on ☎ 020 3117 2520 or

their website: <https://protect-advice.org.uk>

8.0 Questions regarding this policy

Any questions should, in the first instance, be referred to the Monitoring Officer.

9.0 Review

This policy will be reviewed annually.



Anti-Money Laundering Policy 2021/22

A guide to the Council's anti-money laundering safeguards and reporting arrangements

November 2021

Contents	Page
1. Introduction	1
2. Scope of the Policy	1
3. Definition of Money Laundering	1
4. Requirements of the Money Laundering Legislation	2
5. The Money Laundering Reporting Officer (MLRO)	2
6. Client Identification Procedures	2
7. Reporting Procedure for Suspicions of Money Laundering	2
8. Consideration of the disclosure by the MLRO	4
9. Training	5
10. Conclusion	5
11. Review	5

ANTI-MONEY LAUNDERING POLICY

1. Introduction

Although local authorities are not directly covered by the requirements of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, guidance from CIPFA indicates that they should comply with the underlying spirit of the legislation and regulations.

Colchester Borough Council is committed to the highest possible standards of conduct and has, therefore, put in place appropriate and proportionate anti-money laundering safeguards and reporting arrangements.

2. Scope of the Policy

This policy applies to all employees, whether permanent or temporary, and Members of the Council.

Its aim is to enable employees and Members to respond to a concern they have in the course of their dealings for the Council. Individuals who have a concern relating to a matter outside work should contact the Police.

3. Definition of Money Laundering

Money laundering describes offences involving the integration of the proceeds of crime, or terrorist funds, into the mainstream economy. Such offences are defined under the Proceeds of Crime Act 2002 as the following 'prohibited acts':

- Concealing, disguising, converting, transferring or removing criminal property from the UK
- Becoming involved in an arrangement which an individual knows or suspects facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person
- Acquiring, using or possessing criminal property
- Doing something that might prejudice an investigation e.g. falsifying a document
- Failure to disclose one of the offences listed in a) to c) above, where there are reasonable grounds for knowledge or suspicion
- Tipping off a person(s) who is or is suspected of being involved in money laundering in such a way as to reduce the likelihood of or prejudice an investigation.

Provided the Council does not undertake activities regulated under the Financial Services and Markets Act 2000, the offences of failure to disclose and tipping off do not apply. However, the Council and its employees and Members remain subject to the remainder of the offences and the full provisions of the Terrorism Act 2000.

The Terrorism Act 2000 made it an offence of money laundering to become concerned in an arrangement relating to the retention or control of property likely to be used for the purposes of terrorism or resulting from acts of terrorism.

Although the term 'money laundering' is generally used to describe the activities of organised crime, for most people it will involve a suspicion that someone they know, or know of, is benefiting financially from dishonest activities.

Potentially very heavy penalties (unlimited fines and imprisonment up to fourteen years) can be handed down to those who are convicted of one of the offences above.

4. Requirements of the Money Laundering Legislation

The main requirements of the legislation are:

- To appoint a money laundering reporting officer
- Maintain client identification procedures in certain circumstances
- Implement a procedure to enable the reporting of suspicions of money laundering
- Maintain record keeping procedures.

5. The Money Laundering Reporting Officer (MLRO)

The Council has designated the Monitoring Officer as the Money Laundering Reporting Officer (MLRO). He can be contacted at andrew.weavers@colchester.gov.uk or on 01206 282213.

In the absence of the MLRO or in instances where it is suspected that the MLRO themselves are involved in suspicious transactions, concerns should be raised with the Council's Section 151 Officer, Paul Cook.

6. Client Identification Procedures

Although not a legal requirement, the Council has developed formal client identification procedures which must be followed when Council land or property is being sold. These procedures require individuals and if appropriate, companies to provide proof of identity and current address.

If satisfactory evidence is not obtained at the outset of a matter, then the transaction must not be progressed and a disclosure report, available on the Council's intranet (COLIN), must be submitted to the Money Laundering Reporting Officer.

All personal data collected must be kept in compliance with the Data Protection Act.

7. Reporting Procedure for Suspicions of Money Laundering

Where you know or suspect that money laundering activity is taking/has taken place, or become concerned that your involvement in a matter may amount to a prohibited act under the Act, you must disclose this as soon as practicable to the MLRO. The disclosure should be within "hours" of the information coming to your attention, not weeks or months later.

Your disclosure should be made to the MLRO using the disclosure report, attached at Appendix 1 to this policy. The report must include as much detail as possible including

- Full details of the people involved
- Full details of the nature of their/your involvement.

- The types of money laundering activity involved
- The dates of such activities
- Whether the transactions have happened, are ongoing or are imminent
- Where they took place
- How they were undertaken
- The (likely) amount of money/assets involved
- Why, exactly, you are suspicious.

Along with any other available information to enable the MLRO to make a sound judgment as to whether there are reasonable grounds for knowledge or suspicion of money laundering and to enable him to prepare his report to the National Crime Agency (NCA), where appropriate. You should also enclose copies of any relevant supporting documentation.

If you are concerned that your involvement in the transaction would amount to a prohibited act under sections 327 – 329 of the Act, then your report must include all relevant details, as you will need consent from the NCA, via the MLRO, to take any further part in the transaction - this is the case even if the client gives instructions for the matter to proceed before such consent is given. You should therefore make it clear in the report if such consent is required and clarify whether there are any deadlines for giving such consent e.g. a completion date or court deadline.

Once you have reported the matter to the MLRO you must follow any given directions. You must NOT make any further enquiries into the matter yourself: any necessary investigation will be undertaken by the NCA. Simply report your suspicions to the MLRO who will refer the matter on to the NCA if appropriate. All members of staff will be required to co-operate with the MLRO and the authorities during any subsequent money laundering investigation.

Similarly, at no time and under no circumstances should you voice any suspicions to the person(s) whom you suspect of money laundering, even if the NCA has given consent to a particular transaction proceeding, without the specific consent of the MLRO; otherwise, you may commit a criminal offence of “tipping off”.

Do not, therefore, make any reference on a client file to a report having been made to the MLRO – should the client exercise their right to see the file, then such a note will obviously tip them off to the report having been made and may render you liable to prosecution. The MLRO will keep the appropriate records in a confidential manner.

8. Consideration of the disclosure by the Money Laundering Reporting Officer

Upon receipt of a disclosure report, the MLRO must note the date of receipt on his section of the report and acknowledge receipt of it. He should also advise you of the timescale within which he expects to respond to you.

The MLRO will consider the report and any other available internal information he thinks relevant, for example:

- reviewing other transaction patterns and volumes
- the length of any business relationship involved
- the number of any one-off transactions and linked one-off transactions

- any identification evidence held.

The MLRO will undertake such other reasonable inquiries he thinks appropriate in order to ensure that all available information is taken into account in deciding whether a report to the NCA is required (such enquiries being made in such a way as to avoid any appearance of tipping off those involved). The MLRO may also need to discuss the report with you.

Once the MLRO has evaluated the disclosure report and any other relevant information, he must make a timely determination as to whether:

- there is actual or suspected money laundering taking place; or
- there are reasonable grounds to know or suspect that is the case; and
- whether he needs to seek consent from the NCA for a particular transaction to proceed.

Where the MLRO does so conclude, then he must disclose the matter as soon as practicable to the NCA on their standard report form and in the prescribed manner, unless he has a reasonable excuse for non-disclosure to the NCA (for example, if you are a lawyer and you wish to claim legal professional privilege for not disclosing the information).

Where the MLRO suspects money laundering but has a reasonable excuse for non-disclosure, then the MLRO must note the report accordingly; he can then immediately give his consent for any ongoing or imminent transactions to proceed.

In cases where legal professional privilege may apply, the MLRO must liaise with the Council's Section 151 Officer to decide whether there is a reasonable excuse for not reporting the matter to the NCA.

Where consent is required from the NCA for a transaction to proceed, then the transaction(s) in question must not be undertaken or completed until the NCA has specifically given consent, or there is deemed consent through the expiration of the relevant time limits without objection from the NCA.

Where the MLRO concludes that there are no reasonable grounds to suspect money laundering then he shall mark the report accordingly and give his consent for any ongoing or imminent transaction(s) to proceed.

All disclosure reports referred to the MLRO and reports made by him to the NCA must be retained by the MLRO in a confidential file kept for that purpose, for a minimum of five years.

The MLRO commits a criminal offence if he knows or suspects, or has reasonable grounds to do so, through a disclosure being made to him, that another person is engaged in money laundering, and he does not disclose this as soon as practicable to the NCA.

9. Training

Officers considered likely to be exposed to suspicious situations, will be made aware of these by their senior officer and provided with appropriate training.

Additionally, all employees and Members will be familiarised with the legal and regulatory requirements relating to money laundering and how they affect both the Council and themselves.

Notwithstanding the paragraphs above, it is the duty of officers and Members to report all suspicious transactions whether they have received their training or not.

10. Conclusion

Given a local authority's legal position with regard to the legislative requirements governing money laundering, the Council believes that this Policy represents a proportionate response to the level of risk it faces of money laundering offences.

11. Review

This policy will be reviewed annually.

CONFIDENTIAL

Appendix 1

REPORT TO MONEY LAUNDERING REPORTING OFFICER
RE: SUSPECTED MONEY LAUNDERING ACTIVITY

To: Monitoring Officer, Money Laundering Reporting Officer
From: *[Name of employee]*
Department: *[Post title and Service Area]*
Ext / Tel No:

DETAILS OF SUSPECTED OFFENCE:**Name(s) and address(es) of person(s) involved:***[If a company / public body please include details of nature of business]***Nature, value and timing of activity involved:***[Please include full details e.g. what, where, how. Continue on a separate sheet if necessary]***Nature of suspicions regarding such activity:***[Please continue on a separate sheet if necessary]*

Has any investigation been undertaken (as far as you are aware)? *[Please tick relevant box]* Yes ☐ No ☐

If yes, please include details below:

Have you discussed your suspicions with anyone else? Yes ☐ No ☐

[Please tick relevant box]

If yes, please provide details of who the discussions took place with and explain why such discussion was necessary:

Have you consulted any supervisory body guidance re: money laundering (e.g. the Law Society) *[Please tick relevant box]* Yes ☐ No ☐

If yes, please specify below:

Do you feel you have a reasonable justification for not disclosing the matter to the NCA? (e.g. are you a lawyer and wish claim legal privilege?) *[Please tick relevant box]* Yes ☐ No ☐ **to**

If yes, please set out full details below:

Are you involved in a transaction which might be a prohibited act under sections 327-329 of the Act and which requires appropriate consent from the NCA

Yes ☐No ☐

[Please tick relevant box]

If yes, please include details below:

Please set out below any other information you feel is relevant:

Please do not discuss the content of this report with anyone you believe to be involved in the suspected money laundering activity described. To do so may constitute a tipping off offence, which carries a maximum penalty of 5 years imprisonment.

Signed:

Dated:



Code of Practice on Covert Surveillance 2021/22

A guide to the Council's approach to
the Regulation of Investigatory
Powers Act 2000

November 2021

Contents	Page
1.0 INTRODUCTION	1
2.0 WHAT DOES THE ACT AND THE CODE COVER?	2
2.1 Directed surveillance	2
2.2 General observations	2
2.3 Intrusive surveillance	3
2.4 Covert Human Intelligence Sources	3
3.0 AREAS OF OPERATION	4
4.0 AUTHORISATION AND AUTHORISING OFFICERS	4
5.0 CRIME THRESHOLD	5
6.0 GROUNDS FOR GRANTING AN AUTHORISATION	6
7.0 PROCEDURE FOR AUTHORISATIONS, CANCELLATIONS AND RENEWALS	6
7.1 Authorisations	6
7.2 Magistrates' Approval	7
7.3 Review	7
7.4 Renewals	7
7.5 Cancellations	8
7.6 Audit	8
8.0 MISCELLANEOUS POINTS	8
8.1 Material obtained from covert surveillance ("product")	8
8.2 CCTV	8
9.0 SOCIAL MEDIA	8
10.0 TRAINING	9
11.0 GENERAL BEST PRACTICES	9
12.0 SENIOR RESPONSIBLE OFFICER	10
13.0 COMPLAINTS	10
14.0 QUERIES ABOUT THIS CODE OF PRACTICE	10

CODE OF PRACTICE ON COVERT SURVEILLANCE

1.0 INTRODUCTION

The Council enforces the law in a number of areas. As part of this enforcement there will be occasions where surveillance of individuals or property is necessary to ensure that the law is being complied with. When the Council does decide to undertake surveillance, it is important that it remains within the law which is contained in the Regulation of Investigatory Powers Act 2000 ("the Act") as amended by the Protection of Freedoms Act 2012 and the Investigatory Powers Act 2016.

The GOV website provides an overview of the Act and procedures:

<http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/>

The Act sets out certain criteria that the Council has to comply with before it undertakes surveillance and those are also reflected in the Home Office Code of Practice on Covert Surveillance and Property Interference ("the Code of Practice") which is available on its website:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

The Home Office has also issued guidance on the judicial approval process for the Regulation of Investigatory Powers (RIPA) Act 2000 and the crime threshold for directed surveillance. This is available on the Home Office website:

<http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/local-authority-england-wales?view=Binary>

Officers will need to familiarise themselves with the contents of the Code of Practice and the Code.

The Investigatory Powers Commissioner's Office has responsibility for oversight of investigatory powers.

<https://www.ipco.org.uk/>

The Council will comply with the Code when carrying out directed surveillance and officers should be aware of its provisions. Failure to observe the provisions of the Act may result in the protection of the Act not being available. This may mean that the evidence gathered:

- *is not admissible in court proceedings.*
- *is a breach of an individual's human rights.*

This policy sets out how Colchester Borough Council (including Colchester Borough Homes) will comply with the Act, the Code and the Code of Practice. It also clarifies the circumstances in which officers will be able to use covert surveillance and the internal requirements that will need to be observed when conducting that surveillance.

The Policy Statement should be read in conjunction with the Council's Data Protection Policy.

The Policy Statement will be made available for inspection at Council offices.

Any officer considering an application under the Act should first seek the advice of the Senior Responsible Officer in Legal Services.

2.0 What does the Act and the Code cover?

The Act and the Code cover covert surveillance, which is defined in the Act as being surveillance which *"is carried out in manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place"*.

2.1 Directed surveillance

Local authorities can only use a form of covert surveillance called "directed surveillance". This is defined in the Act as where the surveillance is covert but not intrusive and is undertaken:

- for the purposes of a specific investigation or operation
- in such a manner as is likely to result in the obtaining of private information about a person (whether or not specifically identified for the purposes of the investigation) and
- otherwise than by way of an immediate response to events or circumstances, the nature of which is such that it would not be reasonably practicable for an authorisation under the Act to be sought.

"Private Information" in relation to a person includes any information relating to their private or family life.

Surveillance is not covert if notification has been sent to the intended subject of the surveillance. For example, in a noise nuisance case a letter notifying a subject that the noise will be monitored by officers visiting will make the surveillance overt. However, as a matter of good practice, surveillance should be considered covert if the notification to the subject is over 3 months old. All communications of this nature should be sent by Registered Post or delivered by hand.

2.2 General observations

General observations by officers in the course of their duties are not covered by the Act

Directed surveillance will not include surveillance that is undertaken as an immediate response to events or circumstances which, by their nature could not have been foreseen. This will include situations where officers are out in the normal course of their duties and happen to witness an activity, for example a housing officer visiting tenants and witnessing anti-social behaviour by an individual. *In other words, where there is no systematic surveillance.*

If there is any doubt as to whether a RIPA authorisation is required, you must seek advice from the Council's Legal Services.

2.3 Intrusive surveillance

"Intrusive Surveillance" is surveillance that is:

- carried out in relation to anything taking place on any residential premises or in any private vehicle; and
- involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

Intrusive Surveillance cannot be authorised by local authority officers and all officers are strictly prohibited from engaging in Intrusive Surveillance.

2.4 Covert Human Intelligence Sources

The Council is also permitted to use Covert Human Intelligence Sources under the Act. A Covert Human Intelligence Source is someone who establishes or maintains a personal or other relationship for the covert purpose of helping the covert use of the relationship to obtain information. However, at the current time the Council does not consider this necessary and will not use Covert Human Intelligence Sources.

All officers are strictly prohibited from using Covert Human Intelligence Sources.

Unlike directed surveillance, which relates specifically to private information, authorisations for the use or conduct of a Covert Human Intelligence Source do not relate specifically to private information, but to the covert manipulation of a relationship to gain any information. European Court of Human Rights case law makes it clear that Article 8 of the European Convention on Human Rights includes the right to establish and develop relationships. Accordingly, any manipulation of a relationship by a public authority (e.g. one party having a covert purpose on behalf of a public authority) is likely to engage Article 8, regardless of whether or not the public authority intends to acquire private information.

Not all human source activity will meet the definition of a Covert Human Intelligence Source. For example, a source may be a public volunteer who discloses information out of professional or statutory duty or has been tasked to obtain information other than by way of a relationship.

Certain individuals will be required to provide information to public authorities or designated bodies out of professional or statutory duty. For example, employees within organisations regulated by the money laundering provisions of the Proceeds of Crime Act 2002 will be required to comply with the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 and report suspicious transactions. Similarly, financial officials, accountants or company administrators may have a duty to provide information that they have obtained by virtue of their position to the Serious Fraud Office.

Any such regulatory or professional disclosures should not result in these individuals meeting the definition of a Covert Human Intelligence Source, as the business or

professional relationships from which the information derives will not have been established or maintained for the covert purpose of disclosing such information.

Individuals or members of organisations (e.g. travel agents, housing associations and taxi companies) who, because of their work or role have access to personal information, may voluntarily provide information to the police on a repeated basis and need to be managed appropriately. Public authorities must keep such human sources under constant review to ensure that they are managed with an appropriate level of sensitivity and confidentiality, and to establish whether, at any given stage, they could be regarded as a Covert Human Intelligence Source.

Any officer concerned must seek urgent advice from the Senior Responsible Officer.

3.0 Areas of operation

The Council has examined its functions and considers that the following areas may use directed surveillance from time to time. The following is not meant to be an exhaustive list but covers areas where directed surveillance may be necessary in the course of the Council's business.

- Neighbour nuisance and anti-social behaviour
- Protection of Council property
- Licensing enforcement
- Fraud against the Council (including benefit fraud)
- Misuse of Council property, facilities and services
- Enforcement of the planning regime
- Environmental monitoring and control
- Food Safety enforcement.
- CCTV, but more on this later (see 8.2).

However, this is subject to the crime threshold referred to at 5.0 below.

4.0 AUTHORISATION AND AUTHORISING OFFICERS

If directed surveillance is proposed to be carried out, then **authorisation must be sought**.

Under the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003 as amended by the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 and the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2015, the Council considers that the following officers can authorise directed surveillance ("Authorising Officer"):

Chief Executive;
Chief Operating Officer;
Executive Director; and Strategic Director.

Any case involving Confidential Information must be authorised by the Chief Executive.

An Authorising Officer when being requested to authorise directed surveillance must be satisfied that the request is necessary and meets the criteria set down in the Act, the Code and the Code of Practice. An Authorising Officer must not authorise directed surveillance connected with an investigation in which they are directly involved.

Any application to extend or cancel surveillance must also be approved by an Authorising Officer.

Once any application is approved by the Authorising Officer it must be referred to Legal Services who will make an application for approval by a Magistrate.

No directed surveillance may be undertaken by the Council without the prior approval of a Magistrate.

5.0 CRIME THRESHOLD

The Code of Practice states that the Council:

- **can** only grant an authorisation under RIPA for the use of directed surveillance where it is investigating criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco.
- **cannot** authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment.
- **can** authorise use of directed surveillance in more serious cases as long as the other tests are met – i.e. that it is necessary and proportionate and where prior approval from a Magistrate has been granted. Examples of cases where the offence being investigated attracts a maximum custodial sentence of six months or more could include more serious criminal damage, dangerous waste dumping and serious or serial benefit fraud.
- **can** authorise the use of directed surveillance for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco where the necessity and proportionality test is met and prior approval from a Magistrate has been granted.
- **cannot** authorise the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences or to investigate low-level offences which include, for example, littering, dog control and fly-posting.

6.0 GROUNDS FOR GRANTING AN AUTHORISATION

An authorisation for directed surveillance may only be granted if the Authorising Officer believes that authorisation is necessary:

for the purposes of preventing or detecting crime or of preventing disorder and it meets the crime threshold mentioned in 5.0 above.

AND the Authorising Officer must also be satisfied and believe that the surveillance is proportionate to what it seeks to achieve.

The Code advises that following elements of proportionality should be fully considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived mischief;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others;
- that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result; and
- providing evidence of other methods considered and why they were not implemented.

Covert surveillance will only be used for one of the legitimate purposes where sufficient evidence exists to justify the surveillance and the surveillance is the least intrusive method of meeting that purpose. The surveillance itself must be a proportionate response to the issue it is seeking to address. Consideration should be given to alternative methods of resolving the situation or obtaining the evidence sought and this should be documented.

Particular attention should be paid to the effect of the surveillance on the privacy of other persons ("collateral intrusion"). Measures should be taken to avoid or minimise intrusion. Any collateral intrusion should be taken into account when an Authorising Officer is assessing proportionality.

7.0 PROCEDURE FOR AUTHORISATIONS, CANCELLATIONS AND RENEWALS

7.1 Authorisations

An authorisation must be granted by those persons authorised at 4 above. No other person is permitted to authorise directed surveillance.

Authorisations must be in writing on the form attached.

Authorisation cannot be given to operations after they have commenced. Failure to obtain correct authorisation may mean that evidence is not admissible in legal proceedings and may breach a subject's human rights.

The authorisation form must be kept on the relevant case papers and held securely. A copy of the authorisation must be passed to Legal Services to be held on a central file and monitored for consistency of approach of Authorising Officers and validity.

An authorisation period begins on the date and time the authorisation is approved by a magistrate and will cease to have effect (unless renewed) at the end of a period of *three months* beginning with the day on which it took effect.

7.2 Magistrates' Approval

Once an authorisation form has been completed Legal Services will:

- contact the Magistrates' Court to arrange for a hearing
- supply the court with a partially completed judicial application/order form
- supply the court with a copy of the authorisation and any supporting documents setting out the Council's case
- the hearing will be in private and be heard by a single Justice of the Peace.

The Justice of the Peace may decide to either:

- (i) approve the grant (or renewal) of an authorisation; or
- (ii) refuse to approve the grant (or renewal) of an authorisation.

It is preferable for the Authorising Officer also to attend the hearing to give the Bench assistance if necessary.

7.3 Review

Officers should, as a matter of good practice, review authorisations on a regular basis during the course of that surveillance to ensure that the authorisation still meets the criteria. If it does not, the authorisation should be cancelled using the procedure described below. A review form is attached. Officers in charge of investigations will be required to keep a record of these reviews and will submit a record of that review (normally by email) to the Monitoring Officer to be held centrally.

7.4 Renewals

A renewal of an authorisation can be made shortly before it expires and must be done on the form attached. The original should be kept on the case file and a copy passed to the Monitoring Officer for retention centrally. When considering whether to grant a renewal of an authorisation the Authorising Officer will consider the same factors outlined at 5 above. All renewals must be subject of an application to the Magistrates' Court in line with the procedure at 7.2 above.

7.5 Cancellations

The Authorising Officer who last granted or renewed the authorisation must cancel it if s/he is satisfied that the directed surveillance no longer meets the criteria for authorisation. A cancellation should be made on the form attached. The original should be retained on the case file and a copy passed to Legal Services for retention centrally.

Authorisations, renewals and cancellations are subject to monitoring on an annual basis by the Monitoring Officer as to validity under the Act and the Code.

7.6 Audit

At the end of each calendar year each of the Authorising Officers referred to at 4 must provide the Monitoring Officer with a list of all directed surveillance authorised by them throughout that year or provide written and signed confirmation that no such surveillance has been authorised by them

8.0 MISCELLANEOUS POINTS

8.1 Material obtained from covert surveillance ("product")

Material produced as a result of covert surveillance will be secured and transported securely. Where the product obtained is to be used in criminal proceedings the Council must comply with the provisions of the Police and Criminal Evidence Act 1984. In all other cases the treatment of product must follow Council's guidelines on access, retention and storage as set out in the Data Protection Policy.

8.2 CCTV

The Act and the Code will not usually apply to use of an overt CCTV system because the public are aware that the system is in use. However there are circumstances where the system is used for the purposes of a *specific operation or investigation* and in these circumstances an authorisation will be required. If the police assume operational control of the system an authorisation complying with their own procedures must be supplied to the Council. Further information in respect of these procedures can be found in the Council's CCTV Code of Practice, which has been produced in conjunction with Essex Police.

9.0 SOCIAL MEDIA

With the increasing use of social media there is a significant amount of information on an individual's social networking pages. This information might be relevant to an investigation being undertaken by the Council. However, unguided research into the sites of suspects could fall within the remit of RIPA and therefore require authorisation prior to it being undertaken. **You should therefore seek advice from Legal Services prior to undertaking any investigation using social networking sites.**

Where privacy settings are available but not applied the data available on Social Networking Sites may be considered 'open source' and an authorisation is not usually required. However, privacy implications may still apply even if the subject has not applied privacy settings (section 3.13 of the Code).

Repeat viewing of 'open source' sites, however, may constitute directed surveillance on a case by case basis and this should be borne in mind e.g. if someone is being monitored through, for example, their Facebook profile for a period of time and a record of the information is kept for later analysis, this is likely to require a RIPA authorisation for directed surveillance.

To avoid the potential for inadvertent or inappropriate use of social network sites in investigative and enforcement roles, Officers should be mindful of any relevant guidance

and the Council's separate Use of Social Media in Investigations Policy and Procedure attached at Annex 1 of this Policy.

10.0 TRAINING

The Council will ensure that the Officers who are authorising directed surveillance are appropriately trained.

All Authorising Officers and those routinely engaged in directed surveillance have been provided with this guidance, have access to the Code and the standard forms.

This Code of Practice and the standard forms are available in electronic format on the Council's intranet, COLIN.

11.0 GENERAL BEST PRACTICES

The following guidelines are considered as best working practices by all public authorities with regard to all applications for authorisations covered by the Code:

- applications should avoid any repetition of information;
- information contained in applications should be limited to that required by the relevant legislation;
- an application should not require the sanction of any person in the Council other than the Authorising Officer;
- where it is foreseen that other agencies will be involved in carrying out the surveillance, these agencies should be detailed in the application;
- authorisations should not generally be sought for activities already authorised following an application by the same or a different public authority.

12.0 SENIOR RESPONSIBLE OFFICER

The Council's nominated Senior Responsible Officer in accordance with the Code is Andrew Weavers, Monitoring Officer who will be responsible for:

- the integrity of the process in place within the Council to authorise directed surveillance
- compliance with Part II of the Act, the Code and the Code of Practice
- engagement with the Investigatory Powers Commissioner's Office and inspectors when they conduct their inspections, and where necessary, overseeing the implementation of any post inspection action plans recommended or approved by a Commissioner
- assurance that all authorising officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Investigatory Powers Commissioner's Office
- supervising the maintenance of records.

13.0 COMMUNICATIONS DATA

Before considering submitting an application for the acquisition of communications data, all officers must first refer the matter to the Senior Responsible Officer.

Communications Data is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written). Local Authorities are not permitted to intercept the content of any person's communications.

Part 3 of the Investigatory Powers Act 2016 (IPA) replaced part 1 chapter 2 of the Act in relation to the acquisition of communications data and puts local authorities on the same standing as the police and law enforcement agencies. Previously local authorities have been limited to obtaining subscriber details (known now as "entity" data) such as the registered user of a telephone number or email address. Under the IPA, local authorities can now also obtain details of in and out call data, and cell site location. This information identifies who a criminal suspect is in communication with and whereabouts the suspect was when they made or received a call, or the location from which they were using an Internet service. This additional data is defined as "events" data.

A new threshold for which communications data "events" data can be sought has been introduced under the IPA as "applicable crime". Defined in section 86(2A) of the IPA this means: an offence for which an adult is capable of being sentenced to one year or more in prison; any offence involving violence, resulting in substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal; any offence committed by a body corporate; any offence which involves the sending of a communication or a breach of privacy; or an offence which involves, as an integral part of it, or the sending of a communication or breach of a person's privacy.

Further guidance can be found in paragraphs 3.3 to 3.13 of the Communications Data Code of Practice published on the Home Office website:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf


The IPA has also removed the necessity for local authorities to seek the endorsement of a Justice of the Peace when seeking to acquire communications data. All such applications must now be processed through the National Anti-Fraud Network ("NAFN") and will be considered for approval by the independent Office of Communication Data Authorisation ("OCDA"). The transfer of applications between local authorities, NAFN and OCDA is all conducted electronically and will therefore reduce what can be a protracted process of securing an appearance before a Magistrate or District Judge (see local authority procedures set out in paragraphs 8.1 to 8.7 of the Communications Data Code of Practice).

14.0 COMPLAINTS

The Act, the Code and the Code of Practice are subject to monitoring by the Investigatory Powers Commissioner's Office. Any complaints regarding use of surveillance powers should be dealt with initially through the Council's Complaints and Compliments Procedure. If this does not result in a satisfactory outcome for the complainant then they should be referred to:

The Investigatory Powers Tribunal
PO Box 33220
London SW1V 9QZ
Tel: 0207 035 3711
Website : www.ipt-uk.com

15.0 QUERIES ABOUT THIS CODE OF PRACTICE

Any queries regarding this Code of Practice should be referred to the Monitoring Officer, Andrew Weavers by email at andrew.weavers@colchester.gov.uk or  01206 282213

Use of Social Media in Investigations Policy and Procedure 2021/22

A guide to the Council's approach to the use of social media in relation to Regulation of Investigatory Powers Act 2000 investigations.

USE OF SOCIAL MEDIA IN INVESTIGATIONS

POLICY AND PROCEDURES

CONTENTS

	Page
1. Introduction & Background	3
2. Regulation of Investigatory Powers Act 2000 (RIPA)	3
3. What is Meant by 'Social Media' for the purposes of this Policy	4
4. Privacy Settings	5
5. What Is Permitted Under this Policy	6
6. What Isn't Permitted Under this Policy	6
7. Capturing Evidence	7
8. Other IT Tools Available for Investigative Purposes	8
9. Retention and Destruction of Information	8
10. Policy Review	9

1.0 INTRODUCTION & BACKGROUND

- 1.1 Social Media has become a significant part of many people's lives. By its very nature, Social Media accumulates a sizable amount of information about a person's life, from daily routines to specific events. Their accessibility on mobile devices can also mean that a person's precise location at a given time may also be recorded whenever they interact with a form of Social Media on their devices. All of this means that incredibly detailed information can be obtained about a person and their activities.
- 1.2 Social Media can therefore be a very useful tool when investigating alleged offences with a view to bringing a prosecution in the courts. The use of information gathered from the various different forms of Social Media available can go some way to proving or disproving such things as whether a statement made by a defendant, or an allegation made by a complainant, is truthful or not. However, there is a danger that the use of Social Media can be abused, which would have an adverse effect, damaging potential prosecutions and even leave the Council open to complaints or criminal charges itself.
- 1.3 This Policy sets the framework on which the Council may utilise Social Media when conducting investigations into alleged offences. Whilst the use of Social Media to investigate is not automatically considered covert surveillance, its misuse when conducting investigations can mean that it crosses over into the realms of covert and/or targeted surveillance, even when that misuse is inadvertent. It is therefore crucial that the provisions of the Regulation of Investigatory Powers Act 2000 (RIPA), as it relates to covert and directed surveillance, are followed at all times when using Social Media information in investigations.
- 1.4 It is possible for the Council's use of Social Media in investigating potential offences to cross over into becoming unauthorised surveillance, and in so doing, breach a person's right to privacy under Article 8 of the Human Rights Act. Even if surveillance without due authorisation in a particular instance is not illegal, if authorisation is not obtained, the surveillance carried out will not have the protection that RIPA affords and may mean it is rendered inadmissible.
- 1.5 It is the aim of this Procedure to ensure that investigations involving the use of Social Media are done so lawfully and correctly so as not to interfere with an accused's human rights, nor to require authorisation under RIPA, whilst ensuring that evidence gathered from Social Media is captured and presented to court in the correct manner.
- 1.6 Officers who are involved in investigations, into both individuals and business they suspect to have committed an offence, should consult Legal Services if they are unsure about any part of this Policy and how it affects their investigative practices.

2.0 REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

- 2.1 With the increasing use of smartphones and personal devices, there is a significant amount of information on an individual's Social Media pages. This information might be relevant to an investigation being undertaken by the Council. However, unguided research into the sites of suspects could fall within the remit of RIPA and therefore require authorisation prior to it being undertaken. Officers should therefore seek advice from Legal Services prior to undertaking any investigation using Social Media sites.
- 2.2 Officers embarking on any form of investigatory action should always do so with RIPA in mind. Whilst RIPA will not always be relevant to every investigation, it is vital that officers involved in investigative practices against individuals, regularly review their conduct with respect to investigatory actions. Any investigation is capable of evolving from being one that does not require RIPA authorisation, to one that does, at any point.
- 2.3 Accordingly, this Policy should be read in conjunction with the Council's current Code of Practice on Covert Surveillance, as well as the statutory codes of practice issued by the Secretary of State and the Office of Surveillance Commissioners' Guidance.
- 2.4 Instances of repeated and/or regular monitoring of Social Media accounts, as opposed to one-off viewing, may require RIPA authorisation. Advice should be sought from Legal Services where it is envisaged that this level of monitoring will be required in relation to a particular investigation. See paragraph 6.2 below.

3.0 WHAT IS MEANT BY 'SOCIAL MEDIA' FOR THE PURPOSES OF THIS POLICY

- 3.1 Social Media, sometimes also referred to as a Social Network, can take many forms. This makes defining Social Media, for the purposes of this policy, difficult, however there are some facets which will be common to all forms of Social Media.
- 3.2 Social Media will always be a web-based service that allows individuals and/or businesses to construct a public or semi-public profile. Beyond this, Social Media can be very diverse, but will often have some, or all, of the following characteristics;
- The ability to show a list of other users with whom they share a connection; often termed "friends" or "followers",
 - The ability to view and browse their list of connections and those made by others within the system
 - Hosting capabilities allowing users to post audio, photographs and/or video content that is viewable by others

Social Media can include community based web sites, online discussions forums, chatrooms and other social spaces online as well.

- 3.3 Current examples of the most popular forms of Social Media, and therefore the most likely to be of use when conducting investigations into alleged offences, include:

Facebook	Twitter	Instagram
LinkedIn	Pintrest	Tumblr
Reddit	Flickr	Google+

- 3.4 The number and type of Social Media available to the public is fluid. In a given year, many new sites can open whilst some of the more established names can wain in popularity. This Policy will concentrate on Social Media generally and will not make reference to specific sites or services.

4.0 PRIVACY SETTINGS

- 4.1 The majority of Social Media services will allow its users to decide who can view their activity, and to what degree, through the use of privacy settings. Whilst some users are happy, or otherwise indifferent about who is able to view their information, others prefer to maintain a level of privacy.
- 4.2 Depending on their intentions, many users will purposely use Social Media with no privacy setting applied whatsoever. This could be due to the fact that they are actively promoting something, such as a business or event, and therefore require as many people as possible to be able to view their Social Media profile at all times; others may do so for reasons of self-promotion or even vanity. The information publicly available is known as an individual's public profile.
- 4.3 Those individuals with public profiles who operate on Social Media without any, or only limited, forms of privacy settings being activated do so at their own risk. Often, Social Media sites will advise its users through its terms and conditions of the implications of not activating privacy controls, namely that all content they publish or share will be viewable by everyone, including sometimes people who, themselves, do not have an account with that provider.
- 4.4 Whilst the content or information shared by individuals on Social Media remains the property of that individual, it is nonetheless considered to be in the public domain. Publishing content or information using a public, rather than a private setting, means that the individual publishing it is allowing everyone to access and use that information, and to associate it with them.
- 4.5 The opposite of a public profile is a private profile. Some users of Social Media will not wish for their content, information or interactions to be viewable to anyone outside of a very small number of people, if any. In

these instances, users will normally set a level of privacy on their Social Media profiles that reflects what they are comfortable with being made available, meaning that, for example, only friends, family and other pre-approved users are able to view their content or make contact with them through that site.

- 4.6 By setting their profile to private, a user does not allow everyone to access and use their content, and respect should be shown to that person's right to privacy under Article 8 of the Human Rights Act. This does not, however, extend to instances where a third party takes it upon themselves to share information which originated on a private profile on their own Social Media profile. For example, Person A publicises on their *private* Social Media page that they intend to throw a party, at which they will be selling alcohol and providing other forms of licensable activities, despite not having a licence from the Council to do so. Person B, who "follows" Person A's Social Media page, re-publishes this information on their *public* Social Media page. The information on Person A's profile cannot be used, however the same information on Person B's profile, can.

5.0 WHAT IS PERMITTED UNDER THIS POLICY

- 5.1 Whether or not Social Media can be used in the course of investigating an offence, or potential offence, will depend on a number of things, not least of which is whether the suspect has a Social Media presence at all. Investigating offences will always be a multi-layered exercise utilising all manner of techniques, and it is important not to place too high an emphasis on the use of Social Media in place of more traditional investigative approaches.
- 5.2 Further to this, a lack of information on an individual's Social Media profile should not be taken as evidence that something is or is not true. For example, a lack of evidence corroborating an individual's assertions that they were at a particular location on a specific day does not prove that they are being misleading and it is important to consider it only as part of a well-rounded investigation.
- 5.3 For those individuals who do have a presence on Social Media, a lot of what is permitted under this policy for use in investigations will depend on whether they have a public or private profile. As outlined in 4.4 above, where a person publishes content on a public profile, they allow everyone, including those not on that particular Social Media platform, to access and use that information whilst also allowing it to be associated with them.
- 5.4 In practice, this means that things such as photographs, video content or any other relevant information posted by individuals and businesses to a public profile on any given Social Media platform can be viewed, recorded and ultimately used as evidence against them should the matter end in legal proceedings, subject to the usual rules of evidence.

- 5.5 When considering what is available on an individual's public Social Media profile, those investigating an offence, or potential offence, should always keep in mind what relevance it has to that investigation. Only information that is relevant to the investigation at hand, and goes some way toward proving the offence, should be gathered. If there is any doubt as to whether something is relevant, then advice should be sought from Legal Services.

6.0 WHAT IS NOT PERMITTED UNDER THIS POLICY

- 6.1 When it is discovered that an individual under investigation has set their Social Media account to private, Officers should not attempt to circumvent those settings under any circumstances. Such attempts would include, but are not limited to;
- sending "friend" or "follow" requests to the individual,
 - setting up or using bogus Social Media profiles in an attempt to gain access to the individual's private profile,
 - contacting the individual through any form of instant messaging or chat function requesting access or information,
 - asking family, friends, colleagues or any other third party to gain access on their behalf, or otherwise using the Social Media accounts of such people to gain access, or
 - any other method which relies on the use of subterfuge or deception.

Officers should keep in mind that simply using profiles belonging to others, or indeed fake profiles, in order to carry out investigations does not provide them with any form of true anonymity. The location and identity of an officer carrying out a search can be easily traced through tracking of IP Addresses, and other electronic identifying markers.

- 6.2 A distinction is made between one-off and repeated visits to an individual's Social Media profile. As outlined at paragraph 2 above, a RIPA authorisation must be sought in order to carry out directed surveillance against an individual. Whilst one-off visits, or otherwise infrequent visits spread out over time, cannot be considered "directed surveillance" for the purposes of RIPA, repeated or frequent visits may cross over into becoming "directed surveillance" requiring RIPA authorisation. A person's Social Media profile should not, for example, be routinely monitored on a daily or weekly basis in search of updates, as this will require RIPA authorisation, the absence of which is an offence. For further guidance on this point, officers should contact Legal Services.
- 6.3 Regardless of whether the Social Media profile belonging to a suspected offender is set to public or private, it should only ever be used for the purposes of evidence gathering. Interaction or conversation of any kind should be avoided at all costs, and at no stage should a Council Officer seek to make contact with the individual through the medium of Social Media. Any contact that is made may lead to accusations of harassment or, where a level of deception is employed by the Officer, entrapment,

either of which would be detrimental and potentially fatal to any future prosecution that may be considered.

7.0 CAPTURING EVIDENCE

- 7.1 Once content available from an individual's Social Media profile has been identified as being relevant to the investigation being undertaken, it needs to be recorded and captured for the purposes of producing as evidence at any potential prosecution. Depending on the nature of the evidence, there are a number of ways in which this may be done.
- 7.2 Where evidence takes the form of a readable or otherwise observable content, such as text, status updates or photographs, it is acceptable for this to be copied directly from the site, or captured via a screenshot, onto a hard drive or some other form of storage device, and subsequently printed to a hard copy. The hard copy evidence should then be exhibited to a suitably prepared witness statement in the normal way.
- 7.3 Where evidence takes the form of audio or video content, then efforts should be made to download that content onto a hard drive or some other form of storage device such as a CD or DVD. Those CD's and/or DVD's should then be exhibited to a suitably prepared witness statement in the normal way. Any difficulties in downloading this kind of evidence should be brought to the attention of the Council's IT Team who will be able to assist in capturing it.
- 7.4 When capturing evidence from an individual's public Social Media profile, steps should be taken to ensure that all relevant aspects of that evidence are recorded effectively. For example, when taking a screenshot of a person's Social Media profile, the Council Officer doing so should make sure that the time and date are visible on the screenshot in order to prove when the evidence was captured. Likewise, if the evidence being captured is a specific status update or post published on the suspected offender's profile, steps should be taken to make sure that the date and time of that status update or post is visible within the screenshot. Without this information, the effectiveness of the evidence is potentially lost as it may not be admissible in court.
- 7.5 Due to the nature of Social Media, there is a significant risk of collateral damage in the form of other, innocent parties' information being inadvertently captured alongside that of the suspected offender's. When capturing evidence from a Social Media profile, steps should be taken to minimise this collateral damage either before capturing the evidence, or subsequently through redaction. This might be particularly prevalent on Social Media profiles promoting certain events, where users are encouraged to interact with each other by posting messages or on photographs where other users may be making comments.

8.0 OTHER INFORMATION TECHNOLOGY TOOLS AVAILABLE FOR INVESTIGATIVE PURPOSES

- 8.1 Whilst Social Media can be a useful and fruitful means of investigating offences and potential offences, it is by no means the only tool available within the realm of Information Technology. A vast array of other, mostly web-based tools are also at the disposal of those conducting investigations. For example, where there is a website advertising the services of a local business, and there is evidence that this business is engaging in illegal activity, there are IT tools available that can track who is responsible for setting up that website, and so can be a good starting point when trying to link potential offenders to the offending business.
- 8.2 For assistance in identifying which tools may be appropriate, and how best to utilise them, advice should be sought from the Legal Services and or the Council's IT team.

9.0 RETENTION AND DESTRUCTION OF INFORMATION

- 9.1 Where recorded material (in any form or media) is obtained during the course of an investigation which might be relevant to that investigation, or another investigation, or to pending or future civil or criminal proceedings, then it should **not** be destroyed, but retained in accordance with the requirements of the Data Protection Act 2018 , the Freedom of Information Act 2000, and any other legal requirements, including those of confidentiality, and the Council's policies and procedures regarding document retention. Advice should be sought from the Data Protection Officer or the Monitoring Officer.
- 9.2 Personal data gathered by the Council is subject to the Data Protection Act 2018. When considering whether to retain the data, the Council should:
- review the length of time it keeps personal data;
 - consider the purpose or purposes it holds the information for in deciding whether (and for how long) to retain it;
 - ensure that there is a lawful basis for processing the personal data
 - securely delete information that is no longer needed for this purpose or these purposes; and
 - update, archive or securely delete information if it goes out of date
 - ensure that whilst data is held it is kept secure at all times
- 9.3 Due to the nature of Social Media, it is important to remember that when information produced as a hard copy is destroyed in line with this paragraph, that all digital copies of that evidence is likewise destroyed.

10.0 REVIEW

- 10.1 This Policy will be reviewed annually in line with the Council's Code of Practice on Covert Surveillance to ensure that both documents remain current and compliant with relevant legal requirements and best practice guidance.



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



Acceptable Use Policy

August 2021



Customer Business Culture

Acceptable Use Policy

CONTEXT

We must act appropriately with the information we obtain and hold, and with the systems we use and access. How you use our systems, telephony, email and intranet is important for our reputation and the trust of our customers. This Acceptable Usage Policy covers the security and use of all IT equipment. This policy applies to all employees, Councillors, voluntary workers, agency staff and contractors.

APPLICATION OF POLICY

Everyone who uses information and communications technology provided by Colchester Borough Council (CBC) must be aware of these policy statements and the obligations it places upon them.

Colchester Borough Council commits to informing all employees, members, voluntary workers, agency staff, contractors, Councillors and other third parties of their obligations before they are authorised to access systems and information. Other organisations, and their users, granted access to technology managed by the organisation must abide by this policy.

ACCESS TO IT SYSTEMS

- You must not allow anyone else to use your user username and password on any IT system.
- You must not disclose your password to anyone or ask anyone else for their password. If you suspect your password has become known to anyone else, change it immediately and report it to the ICT team.
- You must not leave user accounts logged in at an unattended and unlocked computer.
- You must not attempt to access data that you are not authorised to use or access.
- You must not install, access or modify applications, systems or data without authorisation.
- You must maintain the security of information as defined in the Information Security Policy.
- You must not access other people's email without their permission.
- You must not forward corporate emails to personal email accounts.
- If you receive or view email or other content not intended for you, you must protect its confidentiality.
- You must take care when replying or forwarding to ensure that only relevant parties are included.

PASSWORDS

- You must not use someone else's username and password to access any IT systems.

- You must not leave your password unprotected (for example writing it down or sharing it with another person).
- Passwords must meet the requirements of the Council's Password Policy.
- All CBC devices must be password protected.

BEHAVIOUR

- You must not participate in unlawful, libellous, immoral or offensive activities, including accessing, downloading, storing, creating, copying or disseminating offensive material. This includes, but is not limited to, material of a pornographic, sexual, violent, criminal, racist, sexist or otherwise discriminatory nature. Further, you must not use the systems to perpetrate any form of fraud or piracy.
- You must not publish a website, or any content on a website, that could bring the organisation into disrepute. This includes publishing defamatory or knowingly false material about the organisation, colleagues or customers in any online publishing format.
- Only subscribe to services with your professional email address when representing the Council.
- CBC facilities and identity must not be used for commercial purposes outside the authority or remit of the Council, or for personal financial gain.
- You must not use the internet or email to make personal gains or conduct a personal business.
- You must not use the internet or email to gamble.
- You must not bring the Council into disrepute through use of online 'social networking' activities.
- You must report faults with information and communications technology and co-operate with fault diagnosis and resolution.
- If you use our technology or our internet provision for personal use, the Council takes no responsibility for the security of your personal information. It is recommended you do not carry out personal financial transactions.

DEVICES

- You must not connect any non-authorised device to the network or IT systems.
- You must not store data on any non-authorised equipment.
- In order to comply with Data Protection Legislation, all Council communications must only be made using Council approved applications and devices.

STORAGE

- You must not give or transfer data or software to any person or organisation, without following the Security Policy.
- Documents must not be stored locally (for example on c drive) on a desktop computer or laptop, as they are not backed up and information may be irretrievable if the device fails or is stolen. This includes synchronising SharePoint and OneDrive to a local device without ICT authorisation or on a secured CBC supplied device.

- The use of mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be authorised by the Strategic ICT Manager. Devices will only be authorised if they can be secured through a password or similar encryption. Personal data must not be stored on mobile devices, unless approved by the Strategic ICT manager.

SECURITY AND LICENSING

- You must not attempt to disable or bypass anti-virus, malware or other security protection, and you should take care not to introduce viruses or malware. If you discover a virus or malware, you must notify ICT immediately.
- You must not use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- You must only use software that is appropriately licensed and materials which are not copyrighted, or for which you have been granted use.

WORKING REMOTELY

- Working away from the office must be in line with Colchester Borough Council's remote working policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in clear view in a vehicle.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely.

USE OF SHAREPOINT

- You must not purposely engage in activity that may deprive an authorised user access to a SharePoint resource.
- You must not attempt to access content for which you do not have permission.
- You must not circumvent SharePoint security measures.
- All staff must maintain the supported infrastructure setup by filing the documents via Adding Properties or via the Details menu and not creating folders within folders.
- Site owners are responsible for managing the use of SharePoint in their area and are accountable for their actions.
- Site owners are responsible for the custody or operation of their SharePoint sites and are responsible for proper authorisation of user access.
- Data used in SharePoint must be kept confidential and secure by the user.
- You must ensure that permissions to document libraries are appropriately set and maintained to ensure the security of information.
- Site owners should review the permissions set on their sites at least annually to ensure unauthorised staff do not have access.
- You must ensure that private or personal documents are secured to ensure the security of information.

- Data can be shared with external people/organisations using for example the 'External sharing' SharePoint site. All documents shared must be removed once the need to share has expired. Any special category data shared in this way must be done with the appropriate set up of SharePoint permissions to ensure the security of that data.

USE OF ONEDRIVE

- OneDrive must not be used as a replacement for corporate shared document management, SharePoint.
- OneDrive documents, for example training notes, certificates, 121 meeting notes must not be kept for longer than necessary.

USE OF TEAMS

- Personal data should not be shared via teams messaging. Where possible, work documents should be stored on SharePoint, not Files tab on Teams. Where it is not possible, make sure the permissions for the Files are set appropriately.
- All users should ensure that permissions for documents are set appropriately
- All users should ensure that only permitted participants are added to teams channels
- Care should be taken when screen sharing and/or recording a meeting to make sure that personal data is not disclosed inappropriately. Permission should be sought from all attendees before recording starts.
- Ensure that when making video calls the environment you are calling from and any backgrounds you are using are appropriate for business use.

MOBILE PHONES

- Requests for a mobile phone will be subject to a valid business case being made and management authorisation.
- In order to prevent unauthorised access, devices must be password protected using the features of the device and a strong password is required to access the network.
- The primary reason for being given a work mobile phone is for business purposes. Using the phone for personal calls should not interfere with daily business and wherever possible be made outside of working hours.
- Employees are expected to use the internet responsibly and productively. Excessive personal internet browsing, including social media use, is not permitted.
- Mobile phones should be connected to wi-fi networks where available to prevent excessive use of data and use of the mobile phone to create a hotspot to work from should be used in exceptional circumstances only. Mobile data usage will be monitored and consistent excessive use may lead to suspension of service.
- Calls to premium rate numbers and overseas are not permitted, unless there is a real business need and authorisation has been provided by the relevant Assistant Director.
- You must not use Colchester Borough Council mobile devices for conducting private business.

- Mobile devices may not be used at any time to, store or transmit illicit materials or harass others.
- When driving, staff are expected to comply with the Council's Vehicle User Handbook and the Road Vehicles (Construction and Use) (Amendment) (No4) Regulations 2003, which prohibit the use of handheld mobile devices at all times when driving.
- If your device use is deemed unacceptable, we may cancel your plan and ask for the return of the device.

WHEN AN EMPLOYEE LEAVES

- Line managers must notify the ICT of any leavers or changes to staff roles so that access can be terminated or amended as appropriate.
- All IT equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to the ICT team.

MONITORING

The Council maintains the right to examine any system or device used in the course of its business, and to inspect any data held there.

To ensure compliance with this policy, the volume of internet and network traffic, and the use and content of emails and visited internet sites, may be monitored. Specific content will not be monitored unless there is suspicion of improper use.

It is the employee's responsibility to report suspected breaches of this policy without delay to their line management and to the ICT team.

All breaches of this policy will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with the Council's disciplinary procedures.

POLICY REVIEW

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

FURTHER INFORMATION

For further information contact ict@colchester.gov.uk

VERSION CONTROL

Purpose:	To specify how the Council maintains security
Status:	Draft
Final date:	
To be reviewed:	August 2022



Information Security Policy

August 2021



Customer Business Culture

Information Security Policy

CONTEXT

Information is essential to delivering services to citizens and businesses. Information security refers to the defence of information or information systems from unauthorised or unintended access, destruction, disruption or tampering. It is important that the Council acts appropriately with the information we obtain and hold. Confidentiality, integrity and availability of information must be proportional and appropriate to maintain services, comply with the law and provide trust to our customers and partners.

APPLICATION OF POLICY

Everyone who accesses information the Council holds must be aware of these policy statements and their responsibilities in relation to information security.

Colchester Borough Council commits to informing all employees, voluntary workers, agency staff, contractors, Councillors and other third parties of their obligations before they are authorised to access systems and information and subsequently at regular intervals. Other organisations, and their users, granted access to information held by Colchester Borough Council must abide by this policy.

This policy should be read in conjunction with the Acceptable Use policy and Data Protection policy.

All those who access information may be held personally responsible for any breach or misuse.

INFORMATION SECURITY PRINCIPLES

Information security is the preservation of:

- Confidentiality – ensuring that information is accessible only to those authorised to have access
- Integrity – safeguarding the accuracy and completeness of information and processing methods
- Availability – ensuring that authorised users have access to information and associated assets when required.

ROLES AND RESPONSIBILITIES

The Organisation

- Ensures compliance with law governing the processing and use of information.

The Chief Executive

- Acts as Accountable Officer ensuring that all information is appropriately protected.

Senior Information Risk Owner

- Assures information security within the organisation
- Promotes information security at executive management level
- Provides an annual statement about the security of information assets.

Technology Delivery Manager

- Provides a central point of contact for information security
- Manages the investigation and mitigation of information security breaches
- Supports Information Asset Owners to assess risks and implement controls
- Ensures that staff are not able to gain unauthorised access to Council IT systems
- Ensures the security of the central computer suite, ensuring that access is restricted to staff with specific job functions
- Ensures that all system developments comply with the Council's ICT Strategy. All system developments must include security issues in their consideration of new developments
- Ensures that a third-party specialist routinely reviews network security
- Ensures that no external agencies are given access to any of the Council's networks unless that body has been formally authorised to have access. All external agencies will be required to sign security and confidentiality agreements with the Council.

System Owners

- Ensure they delete or disable all identification codes and passwords relating to members of staff who leave the employment of the Council on their last working day
- Ensure that all system developments must comply with the Council's ICT Strategy. All system developments must include security issues in their consideration of new developments
- Ensure that written backup instructions for each system under their management are produced. The backup copies should be clearly labelled and held in a secure area. Procedures should be in place to recover to a useable point after restart of this back-up
- Ensure that all systems are adequately documented and are kept up to date so that it matches the state of the system at all times.
- Ensure that a Privacy Impact Assessment (PIA) is completed for the use of any new systems or changes to existing systems

Information Asset Owners

- Assess the risks to the information they are responsible for
- Define the protection measures of the information they are responsible for, taking consideration of the sensitivity and value of the information

- Communicate the protection controls to authorised users and ensure controls are followed
- Ensure that a Privacy Impact Assessment (PIA) is completed when data processing changes or before new personal data is collected or processed

All Managers must:

- Ensure their employees are fully conversant with this policy and all associated standards, procedures, guidelines and relevant legislation; and are aware of the consequences of non-compliance
- Develop procedures, processes and practices which comply with this policy for use in their business areas
- Determine which individuals are given authority to access specific information systems. The level of access to specific systems should be on a job function need, irrespective of status
- Ensure that the relevant system administrators are advised immediately about staff changes affecting computer access (for example job function changes, leaving business unit or organisation) so that access may be withdrawn or changed as appropriate
- Ensure that staff are not able to gain unauthorised access to Council ICT systems or manual data
- Ensure all contractors and other third parties to which this policy may apply are aware of their requirement to comply
- Ensure that those users who have access to any part of the Council's Cash Receipting systems whereby they are taking payments either in person or over the phone should only enter card numbers into the relevant Capita payment screens and **under no circumstances** should Card Holder data such as card numbers be written down or copied by anybody as this would breach The Payment Card Industry Data Security Standard (PCI DSS) compliance
- Ensure that if the Council vacates any of its premises, the manager of the service area occupying the premises must undertake appropriate checks of all areas, including locked rooms, basements and other storage areas, to ensure all Council information is removed. Such checks should be documented, dated and signed.

Everyone must:

- Conduct their business in accordance with this policy
- Only access systems and information for which they are authorised
- Only use systems and information for the purposes authorised
- Comply with all applicable legislation and regulations
- Comply with controls communicated by the Information Asset Owner
- Not disclose confidential or sensitive information to anyone without the permission of the Information Asset Owner
- Ensure confidential or special category information is protected from view by unauthorised individuals

- Not copy, transmit or store information to devices or locations (physical or digital) where unauthorised individuals may gain access to it; the security of devices and locations you use are your responsibility
- Protect information from unauthorised access, disclosure, modification, destruction or interference
- Keep passwords secret and do not allow anyone else to use your access to systems and accounts
- Notify the Technology Delivery Manager of any actual or suspected breach of information security policy and assist with resolution
- Co-operate with compliance, monitoring, investigatory or audit activities in relation to information
- Take responsibility for familiarising themselves with this policy and understanding the obligations it places on them
- Reporting any breach, or suspected breach of information security without delay
- When disclosing personal or special category information to customers, particularly over the phone or in person, ensure that they verify their identity. Service areas dealing with customers on a daily basis should have suitable security questions which must always be used
- Always secure laptops and handheld equipment when leaving an office unattended and lock equipment away when leaving the office. Users of portable computing equipment are responsible for the security of the hardware and the information it holds at all times on or off Council property
- Physical security to all office areas is provided through the access control system. Staff should challenge strangers in the office areas without an ID badge. Never let someone you don't know or recognise to tailgate you through security doors
- Staff working from home must ensure appropriate security is in place to protect Council equipment or information. This will include physical security measures to prevent unauthorised entry to the home and ensuring Council equipment and information is kept out of sight. Council issued equipment must not be used by non-Council staff.
- Use of personal devices to access Council systems or data from abroad is not permitted.

ICT is responsible for maintaining the security and integrity of the Council's infrastructure and network by:

- Ensuring all parts of the network, at entry points and internally including wi-fi connections, are secured appropriately, following industry standards
- Ensuring that all user accounts are secured by the use of Multi Factor Authentication (MFA)
- Ensuring that all infrastructure components are secured to industry standards through managed permissions, firewalls and regular security, application and operating system patching
- Ensuring all infrastructure component, server and network devices, have up to date anti-virus application and tools installed
- Maintaining, patching, upgrading and updating via managed ITIL Change Control procedures
- Regularly conducting internal and external penetration tests and ensuring that outcomes are acted on appropriately and within required timeframes
- Ensuring that Global Administration and Administrator accounts are closely monitored and reviewed on a weekly basis
- Enforcing security policies and taking appropriate action when any breach is detected or reported.

MONITORING

The organisation maintains the right to examine any system or device used in the course of our business, and to inspect any data held there.

To ensure compliance with this policy, the volume of internet and network traffic, and the use and content of emails and visited internet sites, may be monitored. Specific content will not be monitored unless there is suspicion of improper use.

It is the employee's responsibility to report suspected breaches of security policy without delay to their line manager and to the ICT team.

All breaches of this policy will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with the Council's disciplinary procedures.

POLICY REVIEW

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

FURTHER INFORMATION

For further information contact ict@colchester.gov.uk

VERSION CONTROL

Purpose:	To specify how the Council maintains information security
Status:	Draft
Final date:	
Review date:	August 2022



Retention Policy

August 2021



Customer Business Culture

Retention Policy

CONTEXT

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 order to carry out its duties. Colchester Borough Council will ensure that it treats all personal information entrusted to it lawfully and correctly.

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). This Retention Policy and the procedures set down in it are reviewed annually to ensure that the Council continues to comply with the requirements of Article 5 (e) of the General Data Protection Regulations (GDPR), *'kept in the form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed'*.

The purpose of this Policy is to ensure that Colchester Borough Council ensures that:

- crucial records can be located and retrieved as required
- records are kept in accordance with legislation
- records are kept in accordance with business requirements
- the best use is made of available storage facilities
- the medium used for each record is the most appropriate.

This policy should be read in conjunction with the Council's Data Protection Policy.

APPLICATION OF POLICY

The Council will ensure that all personal data is retained and disposed of correctly. For the purposes of this policy, personal data can be held in any medium including, but not exclusively, paper documents or files, electronic images and documents, emails, data records within an electronic dataset, other images, video and audio recordings.

In addition to meeting the requirements of Data Protection Legislation, The Freedom of Information (FoI) Act and the Environmental Information Regulations (EIR) require the Council to maintain records management practices that enable it to respond to requests for information as soon as possible and at the latest within 20 working days.

The Retention Schedule is a control document setting out the periods for which records should be retained to meet the operational needs of the Council and to comply with legal and other requirements. This is a 'live' document which is continually updated.

RELEVANT PRINCIPLES OF DATA PROTECTION

Whenever retaining or disposing of personal information the Council will ensure that:

- Personal data is retained only for as long as necessary
- Data is disposed of properly
- All personal data is processed in accordance with the rights of the individual concerned
- Appropriate security is maintained
- The movement of personal data is done in a lawful way, both inside and outside the Council, and that suitable safeguards exist.

DEFINING RETENTION PERIODS

There are a number of considerations that must be made when deciding upon an appropriate retention period.

- Statutory - some retention periods are governed by statute, for example the 'Health and Safety at Work Act 1974' and 'HMRC VAT Notice 700/21: keeping VAT records'. It is therefore essential that any relevant statutory provisions are taken into account when deciding upon a retention period.
- Civil Action - personal data must be retained if it may be needed to defend possible future legal claims. However, linked information that could not possibly be relevant to any claim must not be retained. Personal data must be deleted when a claim could no longer arise. The Limitation Act 1980 imposes various time limits for the taking of legal action.
- DPA, FoI and EIR - if a request for information is made where the records holding that information are due to be destroyed, the destruction of these records must be suspended.
- Data Protection Act - does not specify retention periods. However, the Act does state that where other statutory record retention provisions exist these take precedence. Data controllers are responsible for implementing the DPA and must decide for how long personal data is retained, taking into account the Data Protection principles, business needs, other legal requirements, any professional guidelines, and best or common practice.
- Historical and research - there may be good grounds for keeping personal data for historical, statistical or research purposes.

There is no requirement to keep records of material routinely discarded in the course of any administrative activity such as duplicates, leaflets or other publicity material, rough drafts or ephemera such as sticky notes.

It is an offence to destroy, delete or amend records or data in order to prevent or attempt to prevent the release of information requested under the FoI Act or the EIR. Where the records holding the information requested have been destroyed in accordance with the retention schedule the Council has a duty to explain why the information is no longer held.

ROLES AND RESPONSIBILITIES

Colchester Borough Council will ensure that:

- 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
- A record of personal data processing is kept and maintained, this will include a data classification

Everyone will ensure that:

- Paper files, digital files and other records or documents containing personal and or special category data are kept securely
- Paper files, digital files and other records or documents containing personal and or special category data are destroyed securely
 - Information which could be released under a Freedom of Information (FoI) request – e.g. information that's already publicly available or which wouldn't attract an exemption, cause harm, distress or embarrassment can be disposed of in normal waste bins.
 - Personal data, special category data, confidential information and commercially sensitive data requires secure disposal e.g via confidential waste bins, shredding, destruction of CD etc. ICT can arrange secure disposal of devices such as laptops, phones and removable media.
 - Anyone who is unsure of whether secure disposal is required should contact data.protection@colchester.gov.uk for advice.
- All personal data is kept in accordance with the Council's retention schedule
- Where there is uncertainty around a retention matter ensure that advice is sought from the Data Protection Officer
- The Retention Schedule reflects current legislative requirements for document and records in their care
- The retention of documents and records is fully defined
- Records are accessible and are made available when necessary so that information requests can be responded to promptly
- Records and documents are destroyed or deleted at the end of the retention period in a secure way
- Records are held in accordance with the Data Protection and Freedom of Information Acts and any other relevant provisions.

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

- Provide assurance relating to their compliant destruction of personal data and when requested allow the Council to audit the protection of data held on its behalf.

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

- Advising the Council and its staff on matters relating to the retention and destruction of personal data.

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 with regard to Data Retention
Status:	Draft
Final date:	
To be reviewed:	August 2022



Income & Debt Management Policy

Customer Business

Contents

Introduction.....	3
Policy aims.....	3
Billing and invoicing arrangements	3
Methods of payment	4
Recovery of unpaid debts	5
Council Tax and Business Rates Process	5
Sundry Debts Process	6
Housing Benefit Overpayment Process	7
Enforcement.....	8
Enforcement Agents	8
Attachment of Earnings, Fees or Benefits.....	8
Bankruptcy Proceedings/Liquidation.....	8
Charging Order on Property.....	9
Committal Proceedings.....	9
Money Claim.....	9
Vulnerable customers & financial difficulty	9
Tracing/Searches.....	10
Bad debts.....	11
Complaints and errors.....	11

Appendices

Standard enforcement for Mortgages and Shared Ownership Schemes.....	13
Standard enforcement action for Penalty Charge Notices.....	14

1. Introduction

- 1.1 The Council is being increasingly commercial in every aspect and service. We balance the importance of supporting our vulnerable customers whilst increasing our income and streamlining processes.
- 1.2 It is important that the Council offers a wide range of easy payment methods to our customers which are available 24 hours a day to aid swift payment in a safe and secure way. The options available to our customers are continually reviewed and improved.
- 1.3 The Income and Corporate Debt Teams manage services on behalf of other services and organisations. Specific Service Level Agreements will be in place for these services.
- 1.4 This policy covers the collection and procedures of the following debts:
 - Council Tax
 - Business Rates (NNDR)
 - Housing Benefit Overpayment
 - Sundry Debts (including Commercial Rent)
 - Penalty charge notices
 - Mortgages and Shared Ownership Schemes

2 Policy Aims

- To ensure that the Council bill/invoice, collect and recover all debts in an economic, effective and efficient manner in accordance to legislation and best practice
- To ensure that all customers will be treated fairly and objectively
- To provide consistent guidelines and procedures
- To set out preferred payment options which are cost effective and support prompt payments whilst enabling payments to be made 24 hours a day, 7 days a week
- Advise and assist customers to avoid debt issues before they arise
- Make pro-active contact whenever possible, by text, emails or telephone to ensure early intervention and payment

3. Billing and Invoicing Arrangements

- 3.1 There is a legal duty placed on the Council to bill for Council Tax and Non Domestic Rates (Business Rates) in accordance with legislation. The processes are automated and managed by the Technical Control Team and the Income Team.
- 3.2 Sundry (Commercial) debts are more varied and can be dealt with by the Income Team in liaison with the individual services.
- 3.3 The below table shows the billing and recovery process in terms of team responsibility for the different types of debt.

	<i>Council Tax</i>	<i>Business Rates</i>	<i>Housing Benefit Overpayments</i>	<i>Sundry Debts</i>
<i>Account administration</i>	Council Tax Team	Business Rates Team	Housing Benefit Team	Individual Service Area
<i>Systems Support</i>	Technical Team	Technical Team	Technical Team	Finance
<i>Billing</i>	Technical Team	Technical Team	Technical Team	Income Team
<i>Payment Processing</i>	Income Team	Income Team	Income Team	Income Team
<i>Debt Recovery</i>	Corporate Debt Team	Business Rates Team	Housing Benefit Team	Income Team

For all types of income the following principles must be followed:

- When goods or services are being provided payments should always be made up front of service delivery
- For charges relating to hire of goods or premises a reasonable deposit should be taken on booking to cover any potential damage and the full cost of hire
- Services should always consider the risk of non-payment and should actively monitor customer accounts and payment activities to highlight possible accumulation of debts

4. Methods of payment

4.1 The Council offers the following payment methods:

- Direct debit
- BACS
- Online payments
- Automated telephone line payments

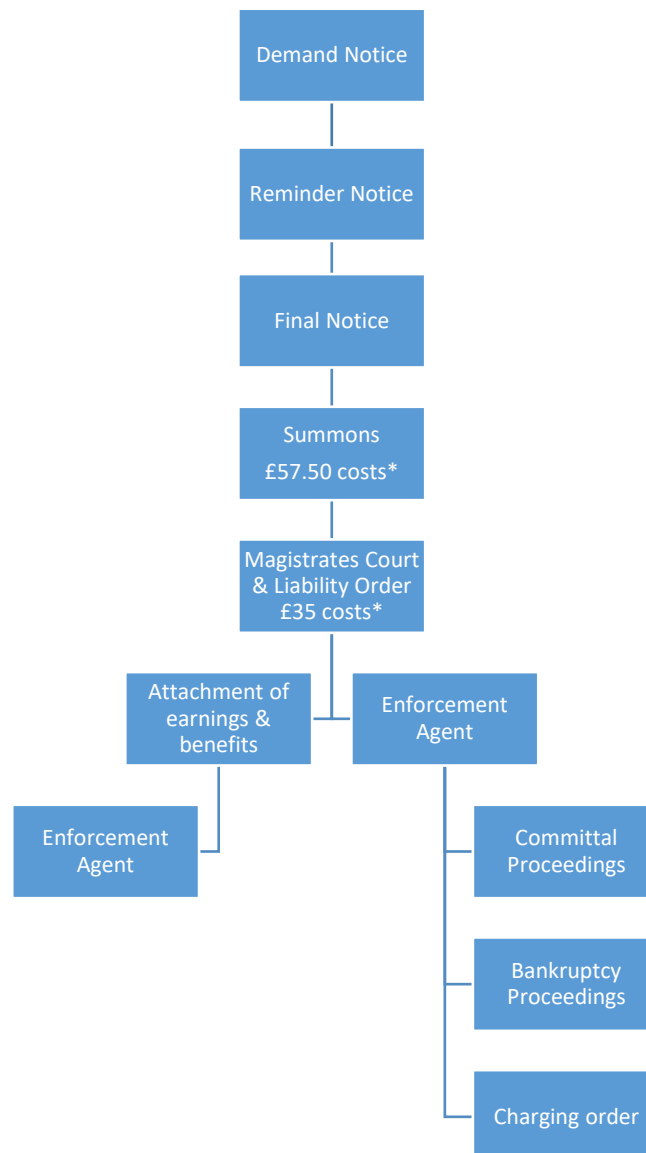
4.3 Services should remove any payment options from promotional materials, bills or other correspondence other than the preferred payment methods. For recurring or regular charges Direct Debit must be promoted as the payment option. For one off charges an upfront debit card internet payment should be promoted followed by other self-serve options.

4.4 It is acknowledged that there may be exceptional circumstances where payments would be received in a method that is not listed above for example if a customer is very vulnerable or if they were in a formal enforcement process.

5. Recovery of unpaid debts

- 5.1 For a variety of reasons, revenue due to the Council will not be paid on time. The Corporate Debt Team and individual services must commence recovery action as soon as possible to maximise the probability of debt recovery.
- 5.2 Reminders will use nudge and persuasive techniques that are most likely to attract prompt payment.

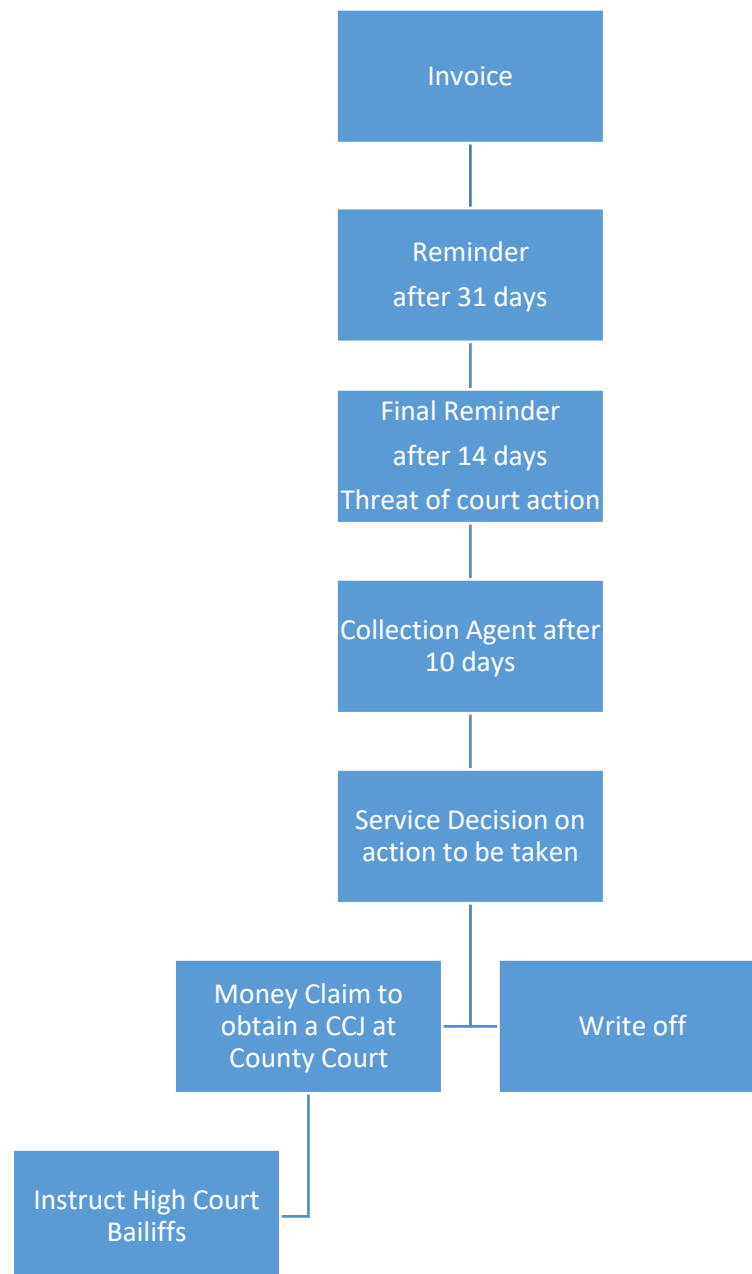
6.1 Council Tax and Business Rates Process



* Please note that Summons and Liability Order costs are subject to review prior to April 2019. The Council calculates the actual cost of issuing the documents and this is recovered as part of the debt. The Council will keep costs to a minimum where possible.

7. Sundry Debt Processes

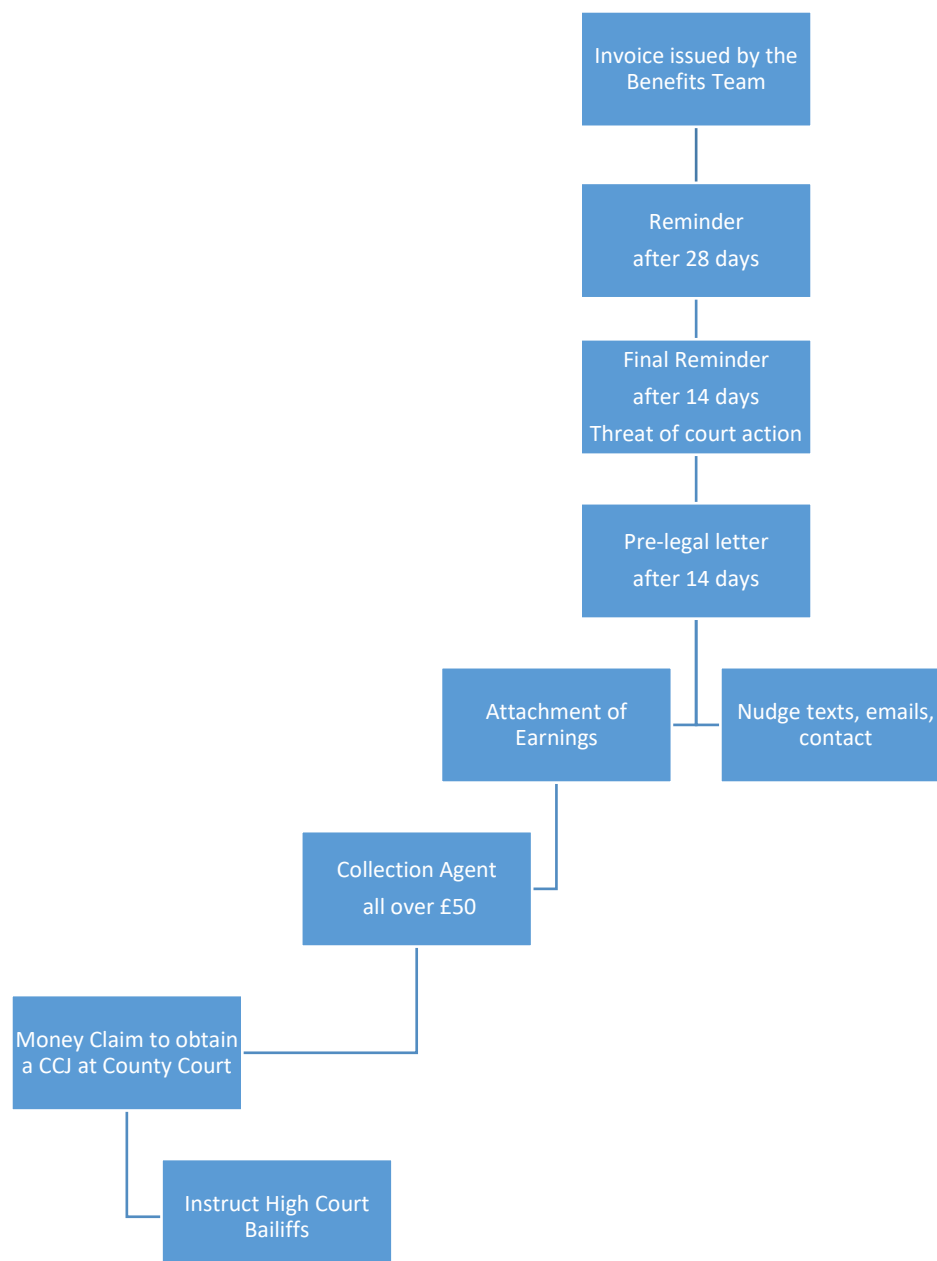
- 7.1 In the cases of sundry debts it is the service or relevant manager who should decide whether enforcement action should be taken. The Income Team will inform services of any debts owing to them and they should respond to say whether each case should then be enforced.



- 7.2 Actions within sundry debt recovery should be complete in a timely manner. Where delays of over 28 days past the due date are encountered at any stage, the reasons should be detailed within the case notes on system.
- 7.3 Forfeiture can also be considered for the recovery of commercial rent. This is where the Council will forfeit a lease due to non-payment of rent. The Council will instruct an Enforcement Agent to carry out the process of securing the property.

8. Housing Benefit Overpayment

- 8.1 A Housing Benefit Overpayment is where an individual has been overpaid benefit for a period that they were not entitled.
- 8.2 A deduction from the claimant's weekly Housing Benefit shall be set following Housing Benefit Regulations. The claimant will receive notification that the overpayment will be recovered in this way.
- 8.3 Where recovery is not possible from existing Housing Benefit an invoice is issued to the claimant or landlord depending on who is liable. The Income Management Team will make use of landlord 'blameless tenant' recovery in cases where the debt is a landlord overpayment and that landlord has other tenants receiving Housing Benefit. The landlord will be notified that we are to recover the overpayment from the claimant and vice versa.



9. Enforcement

- 9.1 The Council will use all means at its disposal to ensure that any debts owed are recovered following any relevant statutory or civil process to enforce payment.
- 9.2 When initiating recovery action the officer must also consider whether the debtor is vulnerable and how any action would impact on them.
- 9.3 The following enforcement options will be considered by Council Officers (as well as other options specific to an individual case):

10. Enforcement Agents

- 10.1 All Enforcement Agents are regulated and have to act in prescribed ways to our customers. They are all fully trained on how to identify vulnerable customers and wear body cameras so all customer contacts are recorded and can be viewed back if required.
- 10.2 There is a clearly defined stage process and Enforcement Agents can only charge fees for each stage when certain trigger actions have been completed.
 - Stage 1- Compliance stage £75.00
 - Stage 2 – Enforcement Stage £235.00 + 7.5% on the original debt over £1,500
 - Stage 3 – Sale Stage £110.00 + 7.5% on the original debt over £1,500

11. Attachment of Earnings, Fees or Benefits

- 11.1 Used where the debtor is employed or in receipt of other regular income where payments can be taken directly from this income. Deductions are made at a rate determined by legislation.

12. Bankruptcy Proceedings/Liquidation

- 12.1 Used when the debtor is a property owner and it is thought that there will be sufficient equity within the property to support full or partial repayment of the debt.
- 12.2 Cases considered suitable for bankruptcy are selected from cases that have been returned from the bailiff, either unable to gain entry or unable to access or returned no goods.
- 12.3 The following factors must be considered:
 - The level of equity available in the liable property and any other associated properties where the debtor has a financial interest must cover the outstanding debt and associated costs
 - Whether the property is up for sale and therefore a charging order would be more appropriate

13. Charging Orders on Property

- 10.1 Used where the debtor owns a property, the Council is able to recover debt when the property is sold in the future. The Council may consider this action where the debtor is on a low income and or is classed as vulnerable or elderly.

11. Committal Proceedings

- 11.1 The law allows Councils to apply to the Magistrates Court to have a person sent to prison where there is culpable neglect or wilful refusal to pay debt.
- 11.2 This will be used when bankruptcy or charging orders are not appropriate. It is not generally accepted by the local magistrates' court as appropriate action, but can be used when other remedies have been exhausted.

12. Money Claim

- 12.1 This is an efficient and inexpensive way for the Council to commence the County Court Judgement (CCJ) process via the County Court. Customers are contacted in regard to any debt by The County Court and given the option to pay in full, set up an arrangement for payment or dispute the debt.
- 12.2 If the judgement is for more than £600 the Council may be able to ask a High Court Enforcement Officer to try to collect the money or remove goods to sell at auction. A warrant is required for this action.

13. Vulnerable customers and those who are in financial difficulty

- 13.2 The Council is committed to support and assist our vulnerable customers. The Income and Corporate Debt Team work closely with the Customer Support Team and external partners to offer the best solution and advice possible for the vulnerable customer and the Council.
- 13.3 Extenuating circumstances will be taken into account when considering recovery action in order to protect the vulnerable and avoid transference of a problem elsewhere.

Considerations may include:

- Whether there are very young or elderly people in the household
- Chronic or terminal illness
- Recent bereavement of spouse or member of household
- Potential homelessness
- The ability of the individual or household to make a payment
- Is an Exceptional Hardship Payment (EHP) or Discretionary Housing Payment (DHP) appropriate

For business debts considerations may include:

- Potential loss of employment for employees of the business
- Loss of key facilities for the local community
- A payment option is the only choice because the business has no assets

- Consideration to any relief that may be appropriate.
- 13.4 Where it has been identified that a customer is suffering from financial difficulties or other extenuating circumstances the Council is committed to providing advice and support as well as a variety of payment options including:
- Holding enforcement action once a customer makes contact to inform of a difficulty in making payment
 - Voluntary payment solutions considered in preference to statutory or civil remedies as a first stage
 - Past history of payments should be considered when making a decision to proceed with enforcement action
 - Where a payment solution is agreed this should be confirmed in writing by the Council including any action that will be taken should the agreed payments not be made
 - Payment solutions should be made with an agreed up-front payment from the debtor whenever possible
 - Where a payment solution cannot be agreed, the debtor will be advised of the reasons why and that the recovery process will continue should an alternative arrangement not be made

14. Tracing and Searches

- 14.1 As part of the recovery process as number of traces and searches can be carried out to try and establish further information on a debtor. This is particularly useful when we have no forwarding address for someone who has moved home before settling a debt.
- 14.2 Locating Council Tax Absconders (LOCTA) is a local government tracing tool that provides a suite of information including, forwarding address, DWP information, credit reports and telephone numbers.
- 14.3 If a LOCTA search is unsuccessful the Council may use a Credit Referencing Agency to trace an individual. The Data Protection Act section 29 allows Local Authorities to credit check and search individuals in regard to the collection of Tax.
- 14.5 The use of internet searches and Social Media to access information in the public domain is also very useful, particularly in establishing employment details for attachment of earnings.
- 14.6 We can also use a Customer Information System (CIS) check that allows certain authorised officers to search DWP database. This information can only be used for the recovery of Housing Benefit Overpayments.
- 14.7 If necessary the Council may ask a Revenues Inspector to carry out a visit to establish the status of a property.

15. Bad debts

15.1 For the purpose of this policy a bad debt is classified as:

- Money due when there is little or no likelihood of recovery after all methods have been exhausted
- Money due where it is uneconomical or inefficient to recover the sum due
- Money due but the debt is too old (aged) to continue recovery
- Money due where the Council does not wish to pursue recovery because the circumstances of a case would attract well-founded adverse publicity or public reaction, or the concept of natural justice would be compromised

15.2 Where it is considered that a debt is a bad debt the Council will ensure that it is written off promptly to preserve and maintain the principle of accurate and up to date information. Decisions will be made based on the circumstances that exist at the time and any unusual circumstances should be referred to the Head of Service or Portfolio Holder.

<i>Debt Value</i>	<i>Process</i>	<i>Authorised Person</i>
Up to £25	Write off on the system with screen notes using write off code	Corporate Debt/Revenues Officer/Housing Benefit Officer
£25 to £100	As above. Income and Corporate Debt Manager to carry out spot checks and record for audit purposes.	Corporate Debt/Revenues Officer Corporate Debt Manager/Housing Benefit Manager
£100 - £5,000	Detailed system checks/searches carried out. If unsuccessful and investigation form is complete and signed. Investigation forms batched and front schedule to be signed.	Corporate Debt Manager/Housing Benefit Manager S151 Officer
Over £5,000	A Portfolio Holder report must be complete with details of individual write-offs	Portfolio Holder

15.3 The cumulative total of debts written off will be monitored by the Income and Corporate Debt Manager to ensure that the incidence of bad debt remains consistent with the Councils estimates and projections.

16. Complaints and errors

- 16.1 If an error or mistake is made in the process of recovering debt the account will be reviewed and appropriate action taken.
- 16.2 If a customer is unhappy with the service provided or disagrees with the decisions made they are able to complain through the Councils standard complaints procedure. Details of this can be found on the Council website - <http://www.colchester.gov.uk/complaints>.
- 16.3 During the process of enforcing payment of outstanding debts it is possible that evidence or facts emerge after enforcement proceedings have been taken or have been completed.
- 16.4 In these cases the Council will take appropriate action to remedy the situation as far as possible:
- Proceedings will be stopped immediately
 - The debtors account will be noted to reflect the revised situation
 - Where appropriate the Court involved will be advised
- 16.5 Although the Council will make every effort to resolve a misrepresentation of the true situation, some issues can only be resolved by reference to the Courts.

Appendix 1

Standard Enforcement Actions for Mortgages and Shared Ownership Scheme

Individual accounts are monitored on a regular basis to ensure that regular monthly payments are received, and reminders sent. Where all or part of the debt is paid by the Pensions Service or the Benefits Division, the receipt of these sums will also be monitored. Whilst standard reminders are available, a more personal approach will often be required.

If the debtor fails to maintain regular payments the Corporate Debt Team will attempt to discuss options. Should this not prove possible, or if arrangements are not adhered to, then the following action will be taken:

Mortgages

Legal Services will be approached and given sufficient information to allow for the preparation of a possession order to be requested from the District Judge. Whilst Court papers are being prepared, Legal Services will warn the debtor of the implications of non-payment.

If a possession order is obtained, the Income Management Team will monitor the arrangement made. Should payment cease, a Portfolio Holder decision will be required if it becomes necessary to implement the order.

Shared ownership cases

Where a mortgage is held on the property, then the lender will be advised that rent is not being paid and that forfeiture proceedings are being considered. If the lender will not make payment on behalf of the borrower, or if there is no lender, the Council will decide whether to pursue forfeiture or to attempt to obtain a money judgment for the County Court.

Appendix 2

Standard Enforcement Actions for Penalty Charge Notices (North Essex Parking Partnership)

This debt is collected directly by the North Essex Parking Partnership and not Customer Services.

Parking enforcement is carried out in accordance with the provisions and procedures laid out in the Traffic Management Act 2004. A parking penalty is not a debt until the motorist has exhausted all avenues of appeal.

- 1. Penalty Charge Notice** issued.
- 2. DVLA enquiry** made if no correspondence received or payment received within 31 days.
- 3. Notice to Owner** sent if full payment is not received within 31 days of issue.
- 4. Charge Certificate** sent and charge increased by 50% of full payment, or representation against Notice to Owner, if not received within 31 days.
- 5. Debt registered at County Court** and fees added if full payment is not received within 17 days of Charge Certificate being sent.
- 6. Order for Recovery** sent.
- 7. Apply for a Warrant of Execution and instruct Enforcement Agents (bailiffs)** if full payment or Witness Statement is not received within 21 days of Notice of Debt Registration being sent. A Warrant of Execution has a lifespan of 12 months only and cannot be reissued thereafter. If the Council has been unsuccessful in recovering the penalty charge by means of a Warrant within 12 months and wishes to pursue, the Council must ask the Traffic Enforcement Centre (Northampton County Court) for authorisation to prepare another Warrant. Warrants that have been returned from the Bailiff after a period of 6 months because the debtor could not be traced or there are no funds or goods to seize can be sent to other Bailiff companies for collection.
- 8.** If warrants remain unpaid, the council is now able to recover debt using a different process where a valid warrant is not required.