Anti-Fraud & Corruption Policy 2016/17

A guide to the Council's approach to preventing fraud and corruption and managing any suspected cases.
DRAFT for committee approval

October 2016

Contents

Page

ANTI-FRAUD & 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 practise 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 & Prevention
- Detection and Investigation
- Awareness & Monitoring

Fraud and corruption are defined as:-

Fraud – "the intentional distortion of financial statements or other records by persons internal or external to the authority, 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 allegation 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 & 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 National and Local Code of Conduct for Members, 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 Strategic Finance Manager 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 & 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 Councils 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 & 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 Procedure Rules 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 his/her 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 Ernst & Young 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 Audit Commission led National Fraud Initiative which is designed to cross match customers across authorities too 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 Ombudsman, HM Customs & Excise and the Inland Revenue. These bodies are important in highlighting any areas where improvements can be made.

5.0 DETECTION & 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 whistle blowing policies.

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 Authority. 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 Code of Conduct for Members then it will be dealt with in accordance with the Arrangement 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 Authority.

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 & 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 2016/17

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

October 2016

Contents

Page

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, Sean Plummer ☎282347

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.

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 & 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) your local Citizens Advice Bureau
(b) relevant professional bodies or regulatory organisations
(c) the police
(d) Local Government 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, Public Concern at Work, can offer independent and confidential advice. They can be contacted on ☎ 020 7404 6609 or by email at whistle@pcaw.co.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 on an annual basis.

Anti-Money Laundering Policy 2016/17.

A guide to the Council's anti-money laundering safeguards and reporting arrangements. DRAFT for committee approval

October 2016

Contents

Page

ANTI-MONEY LAUNDERING POLICY

1. Introduction

Although local authorities are not directly covered by the requirements of the Money Laundering Regulations 2007, 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 on 01206 282213 or at andrew.weavers@colchester.gov.uk

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 Section 151 Officer.

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 Hub, 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, available on the Hub. 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 directions he may give you. 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 e.g.:

- 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;

And 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 he 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.

Code of Practice on Covert Surveillance 2016/17

A guide to the Council's approach to the Regulation of Investigatory Powers Act 2000. DRAFT for Committee approval

October 2016

Contents Page

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.

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 Office of Surveillance Commissioners' Procedures and Guidance in relation to covert surveillance by public authorities ("the Code"). This is available on the Home Office website:

https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

The Home Office has also issued guidance ("the Guidance") on the judicial approval process for RIPA 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 yourself with the contents of the Code and the Guidance.

Other guidance is available on the Office of Surveillance Commissioners website:

(www.surveillancecommissioners.gov.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 Guidance. 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.

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 <u>not</u> 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 should 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.

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 7.2)

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 (these officers are either Chief Officers, Assistant Chief Officers, Assistant Heads of Service, Service Managers or officers in charge of investigations)("Authorising Officer");

Chief Executive
Executive Directors
Assistant Chief Executive Corporate and Financial Management
Head of Commercial Services
Head of Community Services
Head of Customer Services
Head of Operational Services
Head of Professional Services

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 Guidance. 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 Guidance 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 harmful 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 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

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 at any time 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 TRAINING

The Council will endeavour to 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 Hub under One Council/ Corporate Governance/ Code of practice of covert surveillance.

10.0 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.

11.0 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 Guidance;
- engagement with the Office of the Surveillance Commissioners 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.
- that all authorising officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Office of the Surveillance Commissioners.

12.0 COMPLAINTS

The Act, the Code and the Guidance are subject to monitoring by the Office of the Surveillance Commissioners. 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

13.0 QUERIES ABOUT THIS CODE OF PRACTICE

Any queries regarding this Code of Practice should be referred to the Monitoring Officer, Andrew Weavers on ☏ 2213 or by email at andrew.weavers@colchester.gov.uk

Colchester

essexonline

Done Once, Shared By Many

Corporate Information Security Policy

A guide to the Council's approach to safeguarding information resources.

September 2015

Contents

Page

1. Introduction

Information resources are vital to Colchester Borough Council in the delivery of services to residents, businesses and visitors. Their availability, integrity, security and confidentiality are essential to maintain service levels, legal compliance and the public perception of the Council.

It is important that citizens are able to trust the Council to act appropriately when obtaining and holding information and when using the authority's facilities. It is also important that information owned by other organisations which is made available to the Council under secondary disclosure agreements is treated appropriately.

Any public authority which uses or provides information resources has a responsibility to maintain and safeguard them, and comply with the laws governing the processing and use of information and communications technology.

The Chief Executive has ultimate responsibility and endorses the adoption and implementation of this Information Security Policy. Delegated responsibilities are set out in section 6 and rest with Corporate ICT with regard to the maintenance and review of the Corporate Information Security policy, Conditions of Acceptable Use and Personal Commitment Statements as well as local policies.

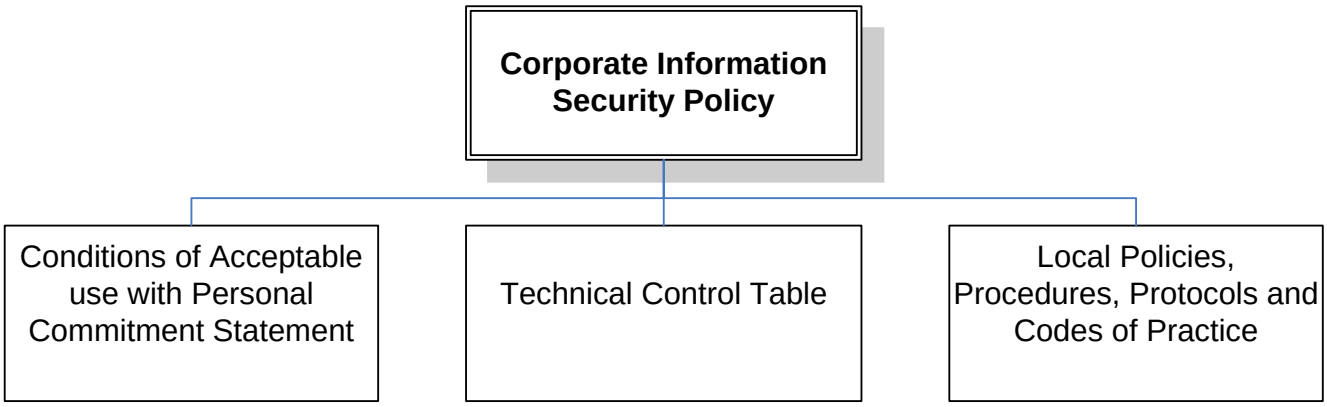
This policy is designed to provide an appropriate level of protection to the information for which the Council is responsible. Supporting this policy is a set of information security technical controls which form the minimum standard that an Essex OnLine partner has to comply with. Individual organisations can strengthen these policies through local policies and procedures, but cannot weaken them.

It is unacceptable for Colchester Borough Council information resources to be used to perform unethical or unlawful acts.

The key aspects of this policy and all associated policies have been developed in accordance with the British Standard for Information security BS7799 – 3:2006 which is harmonised with ISO/IEC 27001:2005.

This Corporate Information Security Policy is supported by further policies, procedures, standards and guidelines. In addition to Council policy, users who are granted access to information owned by other organisations will be subject to the policy requirements of the information owners. Details of these policies will be provided before access is granted.

2. Information Security Framework



3. Objectives

The objectives of the Corporate Information Security Policy are to ensure that:

- All users are aware of these policy statements and associated legal and regulatory requirements and of their responsibilities in relation to Information Security.
- All Council property, including equipment and information, is appropriately protected.
- The availability, integrity and confidentiality of Council information are maintained.
- A high level of awareness exists of the need to comply with Information Security measures.
- Unauthorised access to software and information is prevented.
- The risk of the misuse of email services is reduced.
- The network and network resources are protected from unauthorised access.
- Guidance is provided on handling information of each classification in different circumstances and locations including creation, modification or processing, storage, communication, retention and deletion, disposal or destruction.
- Unwanted incidents such as virus infections, deliberate intrusion and attempted information theft are managed.
- Any unauthorised access, damage and interference to business premises, Information and Information Technology is prevented.

4. Audience

The audience for this policy is for any employee, elected member, agency worker, third party organisation or other authorised personnel. Stakeholders are entitled to view the policy.

5. Legal and regulatory obligations

Colchester Borough Council will comply with all relevant legislation affecting the use of information and communication technology. All users must be made aware of and comply with current legislation as they may be held personally responsible for any breach.

A list of key legislation and regulations, with a brief description of each, and a reference to who in the organisation can provide further information can be found in Appendix A.

6. Roles and Responsibilities

- **Accountable Officer**

The Chief Executive Officer for Colchester Borough Council is ultimately responsible for ensuring that all information is appropriately protected.

- **Information Security Management Group**

This policy has been written by the Essex OnLine Partnership, additional policies, procedures and standards are written by Corporate ICT at Colchester. Corporate ICT are responsible for reviews and approval of Security Policies, which are reviewed and re-issued each year. They are also responsible for approving and overseeing all information security related projects and initiatives. Colchester Borough Council appoints a Senior Information Risk Owner (SIRO) to ensure there is accountability.

The SIRO must provide written judgement of the security and use of the business assets at least annually to support the audit process and provide advice to the Accountable Officer on the content of their statement of internal control.

- **Information Security Management**

This function is fulfilled within the Corporate ICT team who are responsible for the day to day management of information security activities, and for responding to Information Security Incidents. The Head of Security is the ICT Manager.

- **SIRO (Senior Information Risk Owner)**

The SIRO

- Is the officer who is ultimately accountable for the assurance of information security at the Council
- Champions information security at executive management team level
- Owns the corporate information security policy
- Provides an annual statement of the security of information assets (as part of the audit process)
- Receives strategic information risk management training at least once a year

The SIRO is not concerned solely with IT but takes a broader view of our information assets as a whole, in any form.

- **Risk Manager**

The Risk Manager is responsible for the evaluation of the organisation's exposure to risk and controlling these exposures through such means as mitigation, avoidance, management or transference. This role is held by the Corporate ICT team for ICT risks.

- **Information Owners (also referred to as Information Asset Owners)**

The role of Information Asset Owners is to understand what information is held and in what form, how it is added and removed, who had access, and why. They are tasked with ensuring the best use is made of information, and receive and respond to requests about it.

They are responsible for:

- Assessing the risks to the information and data for which they are responsible in accordance with the Risk Management Methodology of the Council.
- Defining the appropriate protection of their information taking into consideration the sensitivity and value of the information.
- Defining the value of information, and identifying the risks associated with the information, so they must classify their information, and define the controls for its protection.

- **Directors, Heads of Service and Line Managers**

Managers are responsible for:

- Ensuring that their employees are fully conversant with this Policy and all associated Policies, Standards, Procedures, Guidelines and relevant legislation, and are aware of the consequences of non-compliance.
- Developing procedures, processes and practices which comply with this Policy for use in their business areas.
- Ensuring that all external agents and third parties acting on behalf of their business area are aware of their requirement to comply.
- Ensuring that when requesting or authorising access for their staff, they comply with the standards and procedures defined by the Information Owners.
- Notifying the Head of Security of any suspected or actual breaches or perceived weaknesses of information security.

- **Employees**

Staff are responsible for:

- Ensuring that they conduct their business in accordance with this Policy and all applicable supporting policies.
- Familiarising themselves with this Policy, and all applicable supporting Policies, Procedures, Standards and Guidelines.
- Responsible for reporting any actual or suspected Information Security Incidents or Problems and assisting with their resolution.

Employees responsible for management of third parties must ensure that the third parties are contractually obliged to comply with this Policy.

- **Users of Systems and Information**

Those who are granted access to Information and information systems must:

- Only access systems and information, including reports and paper documents, to which they are authorised.
- Use systems and information only for the purposes for which they have been authorised.
- Comply with all applicable legislation and regulations.
- Comply with the controls defined by the Information Owner.
- Comply with all Council Policies, Standards, Procedures and Guidelines, and the policies and requirements of other organisations when granted access to their information.
- Not disclose confidential or sensitive information to anyone without the permission of the Information Owner and ensure that sensitive information is protected from view by unauthorised individuals including other people in the same building or location.
- Ensure that, if working from home, adequate physical and other security measures are in place in their homes to prevent any unauthorised access to CBC equipment or information.
- Keep their passwords secret and not allow anyone else to use their account to gain access to any system or information.
- Notify Corporate ICT of any actual or suspected breach of Information Security or of any perceived weakness in the organisation's Security Policies, Procedures, Practices, Process or infrastructure in accordance with the Incident Reporting and Management Procedure.
- Protect Information from unauthorised access, disclosure, modification, destruction or interference.
- Not attempt to disable or bypass any security features which have been implemented.
- Be responsible for reporting any actual or suspected Information Security Incidents or Problems and assisting with their resolution. Corporate ICT are responsible for managing the resolution of each incident and its underlying cause.

7. Approach to Risk Management

Risk management is defined as co-ordinated activities to direct and control an organisation with regard to risk.

The approach of the Council to information security is in accordance with the PSN Risk Management & Accreditation Reference Document as published by the Cabinet Office.

8. Incident Reporting and Management

The Council has established an Incident Reporting and Management framework which is in accordance with the PSN Incident and Problem Management Document as published by the Cabinet Office. That part of this policy is managed by Corporate ICT.

9. Review

The Essex OnLine Partnership must undertake an annual review of Information Security Policies and associated papers to ensure they still comply with current good practice and standards as well as an Equality Impact Assessment if policies change. It is the duty of Colchester Borough Council to review Information Security management arrangements in place and review local arrangements contained within local policies, including an IT Health Check carried out by an accredited independent expert. Accreditation can be with CHECK, an accreditation framework from CESG the Information Assurance (IA) arm of GCHQ, based in Cheltenham, Gloucestershire.

10. Awareness, Compliance and Auditing

The Council will ensure compliance with the Information Security Policy through:

10.1 Awareness

a. Information Security will be included in the induction programme.
b. An ongoing Information Security awareness programme will be implemented for all users including third parties.
c. All users will receive appropriate awareness training and updates in organisational policies and procedures as relevant to their job functions.

10.2 Compliance

Compliance with this Policy is mandatory, and non-compliance with this Information Security Policy, supporting policies, procedures and standards may result in disciplinary action, or termination of contracts under which a business provides services.

10.3 Auditing

a. Carrying out internal audits and where appropriate keeping audit logs in line with legislation and Colchester Borough Council document retention policy.
b. Where connectivity to other secure networks such as N3 or GSi is established, the Council must submit to (and fund) an audit of their security procedures and practices in the form of an annual IT Health Check, and implement any recommendations to demonstrate that they meet the requirements of this security policy.

11. Monitoring

Where appropriate; monitoring arrangements are put in place to ensure compliance with policy objectives, guidelines and standards.

12. Documentation

Document Owners: Essex OnLine Partnership Management Group and Colchester Borough Council

Document Authors: Essex OnLine Partnership Resource Team and Colchester Borough Council

Disclaimer:

A printed version may not be the current version.

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

Version History

Version	Release Date	Update Authorised by	Update carried out by	Update Approved by	Changes
0.1	Oct 2007	EOLP	EOLP Resource Team		First draft
1.0	28th Mar 2008	EOLP	EOLP Resource Team	EOLP Information Security Working Group (ISWG)	Changes agreed by the EOLP Information Security working group on 17-03-08.
2.0	20th Feb 2009	EOLP	EOLP Resource Team	EOLP ISWG	Changes agreed by the EOLP Information Security working group on 05-02-2009.
2.1	30th June 2009	EOLP	EOLP Resource Team	EOLP ISWG	Equality Impact Assessment carried out changes to Section 9 Review to include EQIA and Section 12 Documentation to provide the policy in the required format
2.2	25th Jan 2010	EOLP	EOLP Resource Team		Combined all policies into the Corporate IS Policy and created a set of Technical Control in support of this policy.
2.3	112th Feb 2010	EOLP	EOLP Resource Team		Moved Definitions to Technical Control spreadsheet, minor changes following Information Security working group meeting.

Version	Release Date	Update Authorised by	Update carried out by	Update Approved by	Changes
3.0	1st March 2010	EOLP	EOLP Resource Team	EOLPMG	Removed the highlights that indicated the changes that were made.
3.1	23rd June 2011	EOLP	EOLP Resource Team		Incorporated PSN CoCo requirements
4.0	14th July 2011	EOLP	EOLP Resource Team	EOLP ISWG	Incorporated feedback from ISWG
5.0	27th Sept 2011	EOLP	EOLP Resource Team	EOLP ISWG	Additional text for Information Owners and added role of Risk Manager, text taken from PSS IA glossary. Changes to Approach to Risk and Incident Management
5.1	18th Oct 2012	EOLP	EOLP Resource Team	EOLP ISWG	Risk Manager section changed DSO to SIRO
6.0	Nov 2012	EOLP	EOLP Resource Team	EOLP ISWG	Version 6 Issued
6.1	June 2013	CBC	CBC Information Team		Version 6.1 Issued
6.2	Sept 2014	CBC	Asa Aldis – Information Security Officer		Reference to ISO2700 updated. Reference to Information Team removed
6.3	9 Sep 2015	CBC	ICT Manager	CBC Management	Minor grammatical and formatting changes. Removal of references to the Information Security Officer. Insertion of references to the ICT Manager as Head of Security. Removal of the obligation for ALL users to sign a personal commitment statement.

Appendix A

This is a list of key legislation and regulations.

Data Protection Act 1998 and EU Directive on Data Protection

Personal information relating to identifiable individuals must be kept accurate and up to date. It must be fairly obtained and securely stored. Personal information may only be disclosed to people who are authorised to use it.

Unauthorised disclosure of Council or client personal information is prohibited and could constitute a breach of this Act.

Further information on this Act can be obtained from Corporate ICT: admin.CorporateICT@colchester.gov.uk.

Computer Misuse Act 1990

Deliberate unauthorised access to, copying, alteration or interference with computer programs or data is not allowed and would constitute an offence under this Act for which the penalties are imprisonment and/or a fine.

This Act addresses the following offences:

- Unauthorised access to computer material.
- Unauthorised access with intent to commit or facilitate commission of further offences.
- Unauthorised modification of computer material.

Copyright, Patents and Designs Act 1988

Documentation must be used strictly in accordance with current applicable copyright legislation, and software must be used in accordance with the licence restrictions. Unauthorised copies of documents or software may not be made under any circumstances.

Companies Act 1985

Adequate precautions should be taken against the falsification of records and to discover any falsification that occurs.

Freedom of Information Act 2000

This Act gives a general right of access to all types of data and information that has been recorded by the Council. There are exemptions to the right of access, but the Council must assist applications for information and proactively make details available about the Council. The Council must know what records it holds, where they are stored and must avoid them being lost.

Further information on this Act can be obtained from Corporate ICT: admin.CorporateICT@colchester.gov.uk.

Data Protection Policy 2016/17

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

Draft for committee approval

September 2016

Contents Page

1. Introduction

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

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

2. Statement of Policy

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

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

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

This includes:

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

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

3. The Principles of Data Protection

Whenever collecting or handling information about people the Council will:

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

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

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

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

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

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

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

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

4. Definition of Personal and Sensitive Information

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

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

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

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

5. Roles and Responsibilities

Colchester Borough Council will ensure that:

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

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

All managers and staff will ensure that:

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

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

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

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

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

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

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

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

6. Councillors

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

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

7. The Information Commissioner

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

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

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

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

Disclaimer:

A printed version may not be the current version.

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