CARLOW
COUNTY COUNCIL
COMHAIRLE CHONTAE CHEATHARLOCHA

CARLOW COUNTY COUNCIL

FRAUD PREVENTION POLICY / PREVENTION & AWARENESS GUIDELINES

AND

FRAUD AND CORRUPTION CONTINGENCY PLAN

January, 2019

TABLE OF CONTENTS

1. POLICY STATEMENT

Carlow County Council is committed to the fundamental values of integrity, transparency and accountability. The Council will manage, monitor and control all operations, schemes and projects in such a way that the possibility of fraud and corruption is minimized.

It will investigate thoroughly all cases of suspected fraud and/or corruption and will recover any money and property lost through fraud and/or corruption and pursue prosecutions in cases where it is deemed appropriate.

Depending on the circumstances of an individual case, disciplinary action, in line with the Council's Disciplinary Policy and Procedures, may be initiated against those responsible. Action may also be taken against employees whose lack of supervision/control may have facilitated fraud or corruption.

Signed: _____ ***Date: -*** _____

Kathleen Holohan
Chief Executive

2. DEFINITIONS

FRAUD

For the purpose of this document fraud covers dishonest or illegal acts which result in loss or intended loss, whether financial or otherwise, to Carlow County Council or agents acting on behalf of the Council. Fraud can be committed at all levels within the organization from higher financial transactions to routine day to day activities.

CORRUPTION

Corruption is a specific type of fraud which involves two or more people, where one party offers, gives or accepts any inducement, reward, advantage or benefit, financial or otherwise, which may influence the action of another. There are three main areas of concern with regard to corruption namely; tendering and awarding of contracts, appointment of consultants, planning consents and licences.

Please see Appendix A for further detail

3. PROMOTING AN ANTI-FRAUD CULTURE

Carlow County Council promotes an anti-fraud culture through the following:-

- Any allegation of fraud (anonymous or otherwise) will be investigated.
- Consistent handling of cases without regard to position held or length of service.
- Consideration of whether there have been failures of supervision. Where this has occurred disciplinary action may be initiated against those responsible.
- Losses resulting from fraud will be recovered, if necessary through civil action.
- In general all frauds will be publicized as a deterrent.
- Regularly circulating the Council's anti-fraud policy statement.

4. PREVENTION AND AWARENESS GUIDELINES

4.1. CORPORATE GOVERNANCE

Corporate Governance is the system by which organizations direct and control their functions and relate to their stakeholders. It is the way in which organizations manage their business, determine strategy and objectives and go about achieving those objectives. The fundamental principles are openness, integrity, accountability and effectiveness. At the heart of the organisation's system of Corporate Governance is their Internal Control Framework.

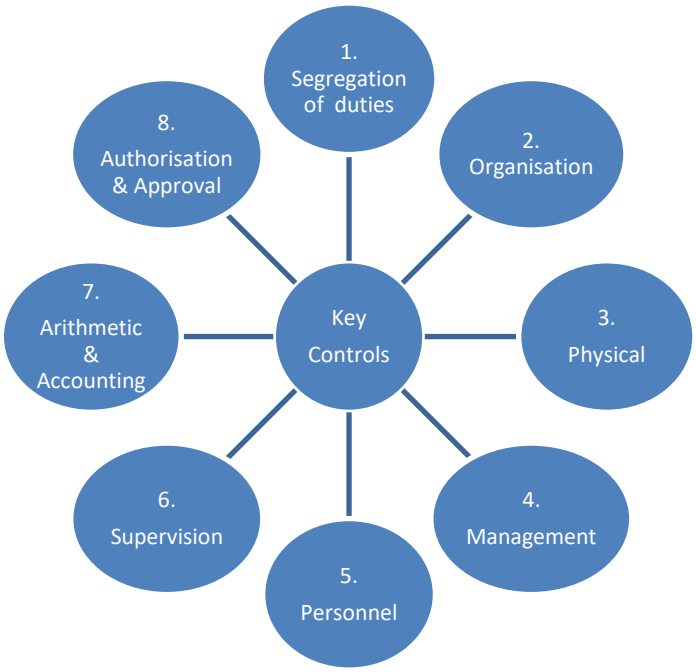
The main components of an internal control framework are:-

- Robust Accountability Structure
- Risk Assessment and Management Processes
- Internal Audit
- Management Policies and Procedures such as:-
  - *Code of Conduct for Employees*
  - *Procurement Policies and Procedures*
  - *Communications Policy*
  - *Grievance and Disciplinary Procedure*
  - *Financial Regulations and Procedures*
  - *Corporate instruments prescribing Regulatory Standards, e.g. County Development Plan*

An internal control framework is defined as being the whole system of controls, financial and otherwise, established by management in order to carry out the business of the organisation in an orderly and efficient manner, ensure adherence to management policies, safeguard assets and secure as far as possible the completeness and accuracy of the records. The individual components of an internal control system are known as *"internal controls".*

4.2. INTERNAL CONTROLS

Internal controls form part of the management system within Carlow County Council. Their purpose is to provide a secure framework and reduce the risk of fraud or corruption occurring. The methods of control, common to all areas, which should be reviewed regularly are outlined hereunder:-



i. **SEGREGATION OF DUTIES**

A key control area is the separation of responsibilities or duties which if combined would enable any one individual to have full control and authorization of an operational area. Segregation of duties reduces the risk of intentional manipulation or error and increases the element of checking. Where segregation of duties is not feasible, this will be managed through closer supervision and/or alternative controls.

ii. **ORGANISATION**

The organization defines and allocates responsibilities and identifies lines of reporting for all aspects of the organisation's operations, including controls. The delegation of authority and responsibility will be clearly specified.

iii. **PHYSICAL CONTROLS**

Procedures and security measures will be reviewed on a regular basis at department level, to ensure that access to assets and the payment offices are limited to authorized personnel. The appropriateness of controls in place in the case of valuable, portable or desirable assets will also be reviewed.

iv. **MANAGEMENT CONTROL**

Management has responsibility for the overall control of the organisation's activities, including reviewing business plans and budgetary control and ensuring adherence to corporate policies etc.

v. **PERSONNEL CONTROLS**

Where possible, procedures will be put in place for the recruitment and selection of employees and subsequent training for carrying out duties and responsibilities. Employee mobility will be encouraged.

vi. **SUPERVISION**

All areas of operations are subject to checking by supervisory personnel. The level of supervision is relevant to the inherent risk of the activity being supervised and prescribed procedures for local supervisors will be determined by management at department level.

vii. **AUTHORISATION & APPROVAL**

All transactions require approval by an appropriately responsible person and this must be communicated and implemented.

viii. **ARITHMETIC AND ACCOUNTING**

All financial transactions must be approved by an authorized person. It is the responsibility of the authorized person to ensure that the transactions are adequately recorded and the proper approvals and processes are in place.

Please see Appendix B for further detail

5. RISK ASSESSMENT AND MANAGEMENT

Risk is the threat that an event, action or failure to act will adversely affect an organisation's ability to achieve its objectives or successfully execute its strategies. Risk management is the process by which risks are identified, evaluated and controlled.

The risks to be addressed as part of a risk management programme are wide ranging and include strategic, operational, financial and reputational risk. A risk strategy does not mean that sensible risks should not be taken, but they should be properly assessed and managed. In Carlow County Council a risk register is prepared in respect of each of the Directorates.

The register records the following information for each objective:-

- A description of the risk
- Any mitigating actions being taken or controls in place
- An assessment of the impact of the likelihood of the risk happening
- An assessment of the impact if the risk were to happen
- Further actions considered necessary to manage the risk or its impact
- The person responsible for taking the actions

The risk register will be a primary tool for risk tracking and will contain the overall system of risks and the status of any risk mitigation actions.

Fraud and corruption are elements which alone, or in combination, have the potential to give rise to risk. There are six broad categories of risk which need to be examined when developing a system of internal controls:-

- Financial
- Operational
- Physical
- External
- Personnel
- Information Technology

Please see Appendix C for further detail

6. GENERAL DATA PROTECTION REGULATIONS (GDPR)

GDPR came into effect on the 25th May, '18. The principal aim of the Regulations is to further enhance the rights of the individual with regard to the processing of personal data. There are two main types of data referred to in GDPR : Personal Data and Special Category Data.

PERSONAL DATA

Personal data is data that relates to or can identify a living person, either by itself or together with other available information.

SPECIAL CATEGORY PERSONAL DATA

Processing of personal data, revealing any of the following, shall be prohibited unless it comes under the exemptions in Article 9.

- Ethnic or racial origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Processing of genetic data
- Biometric data for the purposes of identifying a living person
- Mental or physical data
- Sexual life or orientation

The Council should be cognisant of the following to ensure compliance with GDPR:-

Awareness	Ensure decision makers and key people in the organisation are aware of the implications of GDPR
Information	Documentation of personal information the Council holds, including identifying the source of information and how it is stored
Communicating privacy information	Ensure privacy statements are reviewed
Individuals' rights	Procedures are checked to ensure they cover all the rights of individuals, including how you would delete personal data or provide data electronically
Subject access requests	Procedures are updated and requests are met within the new timeframe (30 days)
Lawful basis for processing data	The lawful basis for processing data is identified, documented and the privacy notice is updated to explain it
Consent	How the Council seeks, records and manages consent should be reviewed. Existing consents should be refreshed if not GDP R compliant
Children	Update systems in place to verify individual ages and obtain parental or guardian consent where necessary
Data breaches	Ensure procedures are in place to detect, report and investigate a personal data breach
Data Protection Impact Statements	Ensure the Council is aware of how and when to implement Data Protection Impact Statements
Data Protection Officers	Ensure an individual is designated to take responsibility for data protection compliance

7. CYBER SECURITY

Cyber security is an integrated approach to preparing, protecting, detecting and responding to cyber threats. It refers to the technologies, processes and practices, both digital and human, designed to protect IT networks, programs and data from attack, damage, compromise or unauthorised access. Carlow County Council uses a proactive prevention approach. Effective prevention requires a layered approach, capable of addressing not only today's threats, but preventing tomorrow's as well. The Council use a number of different software products in their solution, eg the Firewall solution sets up a series of roadblocks that prevent attacks at their initial entry points.

There are a number of spam filters in operation that provide email filtering services for content and attachments. Spam filters keep unwanted email spam from reaching the network. They manage data entering and leaving the network via email. All inbound/outbound email is scanned. To further protect against cyber threats, all links with emails are scanned for threats. If the link is safe, you will be brought to the website. If it is a compromised link, you will not be able to proceed.

Usernames/Passwords

The use of usernames and passwords are a critically integral part of any operating system. Users should be cognisant of their responsibilities with regard to maintaining the secrecy of both their usernames and passwords.

Mobile Device Management

MDM (Mobile Device Management) is software which manages, secures and supports smart mobile devices deployed throughout Carlow County Council. Security is a common challenge for IT departments as mobile devices, primarily smartphones and tablets, become key productivity tools in the workplace. Protecting mobile devices is critical because of the corporate data that could potentially be stored on them. Remotely securing the devices, including taking preventative action when the devices are lost or stolen is an important component.

The full functionality of MDM is only supported by certain handsets. Therefore, all handsets must be secured through the ICT Department to ensure compatibility. The County Council is not in favour of a Bring Your Own Device (BYOD) approach. All smarthphones will have a password policy which requires the user to have a password/pin on every device. This is to ensure that employee carelessness does not become the weakest link in the security implementation. The MDM platform currently deployed in Carlow County Council is Microsoft Intune.

8. ROLES AND RESPONSIBILITIES

The potential for fraud and/or corruption can be curtailed where the Chief Executive and Management Team cultivate within the Council a culture where:-

- Senior officers and leaders provide leadership and good example
- A strong control environment has been developed
- Probity and propriety are manifest in procedures
- A high level of transparency and accountability exists

THE ROLE OF THE CHIEF EXECUTIVE

It is the responsibility of the Chief Executive and the Head of Finance to take all reasonable measures to prevent and detect fraud and corruption.

The Certificate of the Chief Executive/Head of Finance on page 6 of the Annual Financial Statement (as signed by both parties) certify that the financial statements are in agreement with the books of account and accounting requirements and also states that *"we have also taken reasonable steps for the prevention and detection of fraud and other irregularities".*

In addition the Chief Executive will:-

- Ensure there is pervasive awareness within the Authority of the procedures in relation to fraud and/or corruption
- Make it clear that there is a clear commitment to the prevention of fraud and/or corruption and that it will be dealt with seriously, if uncovered
- Guarantee that concerned employees, or members, will be supported and that reprisals will be vigorously defended against

THE ROLE OF ELECTED MEMBERS

As elected representatives, all members of the Council have a duty to the general public to protect the Council and public money from fraud and corruption. The Local Authority Code of Conduct for Councillors imposes a statutory duty on members to maintain proper standards of integrity, conduct and concern for the public interest.

In carrying out their roles Members should:-

- Act in a way which enhances public trust and confidence
- Avoid conflict of interest and never seek to use improper influence
- Make decisions based on consideration of the public interest and the common good[1]
- Promote equality and avoid bias
- Perform their functions in a responsible and diligent manner
- Maintain proper standards of integrity, conduct and concern for the public interest[2]
- Complete a "*declaration of interest"* each year[3]

THE ROLE OF DIRECTORS OF SERVICES

It is the responsibility of the Directors of Services to take such steps as are reasonably available to them to prevent and detect fraud and corruption. This includes:-

- Management/Directors are expected to create an environment in which they may be easily approached by employees with any concerns relating to suspected irregularities
- Ensuring employees understand their responsibilities through adequate training, supervision, written procedures and job descriptions
- Frequently updating and reviewing the Risk Register by examining risks within their remit
- Ensure effective controls are developed and maintained
- The communication and implementation of this policy in their work area
- Ensure that all employees are aware of the Council's personnel policies and procedures
- Taking steps to provide reasonable assurance that the activities of the organization are conducted honestly and that its assets are safeguarded
- Examine the need to rotate employees at all levels in areas with a potential of fraud
- Ensure that agreed internal audit recommendations are expeditiously addressed and implemented
- Ensuring, that to the best of their knowledge and belief, financial information whether used in the entity or for financial reporting is reliable
- Delegate responsibilities and ensure compliance from employees
- Ensure regular reviews of controls are carried out to take into account any change in procedures or new schemes/projects

[1] S170, Part 15 Local Government Act, '01, prohibits elected members from seeking, demanding or accepting from any person any favours, rewards, remuneration, for any action or inaction by virtue of employment or office held

[2] The Local Authority Code of Conduct for Councillors imposes a statutory duty on members to maintain proper standards of integrity, conduct and concern for the public interest.

[3] Elected members are required to complete *"declaration of interest"* each year in accordance with Part 15 of the Local Government Act, 2001.

THE ROLE OF EMPLOYEES

The Code of Conduct for employees should be adhered to at all times. The core values underlying the Code include honesty, impartiality, integrity and serving the common good. Employee awareness of policy and procedures are fundamental to the effective operation of systems. Employees should:-

- Ensure the safeguarding of public funds or assets entrusted to them
- Inform Line Managers of any gifts/hospitality offered
- Alert Line Managers to fraud or suspected fraud
- Assist in any investigation that may arise in respect of fraud or suspected fraud
- Inform Line Managers of any outside interests that may conflict or impinge on their duties
- Make management aware of any concerns they have about the conduct of Council affairs or the use of Council assets and resources
- Employees are required to make a *"declaration of interest"*[4]
- Employees are prohibited from accepting favours, rewards etc for any action/inaction by virtue of employment or office held[5]

THE ROLE OF LINE MANAGERS AND SUPERVISORS

Line Managers and supervisors are expected to set example by complying fully with procedures and controls and be alert to the fact that an operational area is exposed to fraud and corruption. Line Managers and Supervisors must ensure that:-

- Their areas are risk managed and working within a controlled environment
- Controlled procedures are regularly reviewed
- Employees are briefed on common types of fraud that can occur
- Procedure Manuals and checklists should be available for employees
- Employees are rotated where necessary
- Line managers/supervisors should actively check that their employees are complying with procedures
- Line managers/supervisors should monitor employee usage of the Council's email, equipment/resources, phone and internet and ensure compliance with the relevant policies

[4] All relevant employees are required to complete a *"declaration of interest"* each year as per Part 15 of the Local Government Act, 2001

[5] Section 170, Part 15, of the Local Government Act, 2001, prohibits an employee, member of the local authority or of a committee of a local authority from seeking, demanding or accepting from any person other than the local authority concerned, favours, rewards, remuneration or fees for any action or inaction by virtue of employment or office held.

THE ROLE OF HUMAN RESOURCES

A key preventative measure to deter fraud and corruption is to take effective steps at the recruitment stage to establish, as far as possible, the previous record of potential employees in terms of their propriety and integrity.

Human Resource's responsibilities are:-

- Ensure that employees appointed by the Council are of good character
- Ensure detailed appraisal of employees during probationary periods
- Issue new employees with the Council's Code of Conduct on appointment
- Have appropriate disciplinary procedures in place
- Monitor sick leave patterns, areas of high employee turnover and annual leave patterns
- Put in place an employee mobility policy
- Ensure fraud awareness is included in training programmes for employees at all levels

THE ROLE OF INTERNAL AUDIT

Internal Audit plays an important preventative role in providing reasonable assurance that appropriate systems and procedures are in place to prevent and deter fraud and corruption. Internal Audit assists management by:-

- Independently reviewing systems, procedures and controls to ensure that there are adequate safeguards to prevent, deter and detect fraud and corruption
- Advising managers on appropriate controls to put in place
- Assisting in the deterrence and prevention of fraud by examining and evaluating the effectiveness of controls applied in different Departments
- Identifying areas of concern, through carrying out specific audits and testing of systems
- Independently investigating suspected frauds and irregularities and reporting conclusions to management

THE ROLE OF THE AUDIT COMMITTEE

The Audit Committee shall ensure that procedures are in place whereby employees may in confidence raise concerns about possible irregularities in financial reporting or financial matters in accordance with the Protected Disclosures Act, 2014.

9. EMPLOYEE SUPPORT

It is not uncommon for employees who work closely with the suspected perpetrator to feel a sense of responsibility for what happened and suffer stress as a result. Often there is a feeling of shock and disappointment that a person in whom trust was placed has deceived those around him/her. In these circumstances, employee support may provide a confidential service offering help, advice and support.

10. ABUSE OF THE PROCESS

We must ensure that any investigative process is not misused and, therefore, any abuse such as raising unfounded malicious allegations against a colleague will be dealt with as a disciplinary matter.

11. CONCLUSION

Carlow County Council is committed to tackling fraud and corruption whenever it happens. The Council's response will be effective and organised and will rely on the principles included in this document.

This document will be regularly reviewed to ensure its effectiveness.

FRAUD AND CORRUPTION CONTINGENCY PLAN

(I) DISCOVERING AND REPORTING FRAUD AND CORRUPTION

The objectives of this response plan are to provide a documented framework, to which employees and elected members in Carlow County Council can refer to in the event that fraud and corruption is suspected or reported.

(II) WHAT EMPLOYEES SHOULD DO IF THEY SUSPECT FRAUD OR CORRUPTION

The following are some guidelines for employees on what they should do if they suspect fraud or corruption is happening in their area of work.

- Report any case of suspected fraud or corruption to their line manager.
- Do not attempt to confront or interview suspects *(this is a specialised area and will have implications in any subsequent legal proceedings)* or to contact An Garda Siochana as this is a matter for senior managers to initiate.
- If for any reason, it is not possible or appropriate to inform your line manager, then you should contact the Head of Finance, Internal Auditor or the Senior Executive Officer, Corporate Services, who have been designated by the Chief Executive as the officials to undertake this role.
- Employees may also make a Protected Disclosures pursuant to the terms of Carlow County Council's " Protected Disclosures Policy and Procedures" or Carlow County Council's Audit Committee "Receipt of Protected Disclosures Policy".

(III) INVESTIGATION

- In the case of suspected fraud, the Chief Executive or Head of Finance may direct Internal Audit to carry out an investigation.

- Where particular expertise may be required to assist in an investigation, the Chief Executive or Head of Finance may direct employee(s), or an outside Body, with necessary expertise to assist Internal Audit with any investigation.

- Employees involved in the investigation will ensure that quick and effective action is take to:-
  - Prevent further losses (this may involve changing employee/reallocating jobs)
  - Identify perpetrators
  - Safeguard evidence
  - Minimise adverse publicity and protect Carlow County Council's reputation
  - Rectify weaknesses in the system

- The scope of the investigation may be limited until there is sufficient evidence to support the suspicions

- Details of the report of the suspicion of fraud or corruption should be recorded immediately along with the reasons that gave rise to the suspicions to clarify whether a genuine mistake was made or an irregularity occurred. Employees should be aware that all irregularities will be investigated.

- As part of an investigation, Internal Audit may require to interview employees. Internal Audit investigations will be mindful of the provisions of Carlow County Council's Disciplinary and Grievance Procedure and will liaise with the Senior Executive Officer, Corporate Services, in this regard. Employees will be informed of their right to a trade union or other representative at the interview.

- In the case of major fraud and corruption, the suspected perpetrator may be suspended while the investigation is in progress. Suspension does not imply guilt, but is a safeguard to protect Carlow County Council from any loss or damage of evidence.

- It is the responsibility of the Human Resources function to take forward any disciplinary action which may be required as a result of an investigation. Action may also be taken against employees whose lack of supervision/control may have facilitated the fraud or corruption.

- All cases will be handled consistently, irrespective of grade or length of service.

(IV) OUTCOME

At the conclusion of an investigation, a report will be forwarded to the Chief Executive, regardless of the outcome. The Chief Executive will decide whether the matter should be referred to An Garda Siochana.

The report to the Chief Executive will include:-

- Details of the fraud/corruption irregularity
- Details of how the fraud/corruption irregularity occurred
- Losses/affect on Carlow County Council quantified
- Perpetrator identified
- Action required to prevent a reoccurrence
- Details of any lack of supervision or control weaknesses which may have contributed to the fraud or corruption
- Recommendations for recovery of losses

- Recommendations for referral to Senior Executive Officer, Corporate Services, for any disciplinary action required for either the perpetrator or employees responsible for lack of supervision and control

APPENDIX A

FRAUD AND CORRUPTION

INTERNAL FRAUD EXAMPLES INCLUDE:-

- Payment of false invoices
- Failure to record/account for monies received
- Dealing inappropriately with claims/submissions
- Collusion
- Forgery
- Override controls so as to benefit oneself or another
- Misrepresentations being made to the auditor
- Falsification or alteration of accounting records or other documents
- Misappropriation of assets or theft
- Failing to record any leave type on the leave system in operation
- Falsification of travel and subsistence and/or any other expense claims
- Recording of transactions without substance
- Intentional misapplication of accounting policies
- Misuse of Council's Credit Card

EXTERNAL FRAUD EXAMPLES INCLUDE:-

- False statement(s) in grant applications
- False invoices for payments
- False, or exaggerated, compensation claims

This list is not exhaustive

EXAMPLES OF CORRUPTION

- Accept or solicit a bribe
- Leaking of confidential information which may directly, or indirectly, influence the action of any person
- Collusion to steal, or misuse, Carlow County Council's resources
- Improper or unauthorised use of funds and/or assets
- Office holder acts in an official capacity for his/her own personal gain
- Arrange for a colleague, or any other person, to record you clock in's/out's in order to disguise the fact that you were not present at work

This list is not exhaustive

APPENDIX B

CONTROLS TO PREVENT OR DETECT FRAUD

The risk of fraud can be reduced through the implementation of a robust and comprehensive system of controls on the various underlying accounting, financial and operational transactions of the Council. Individual controls are preventive, detective or corrective in action. The following key areas of control should be examined and reviewed for each and every process within the Council.

- **SEGREGATION OF DUTIES (PREVENTIVE)**
  A key control area is the separation of responsibilities or duties which, if combined, would enable any one individual to have full control and authorisation of an operational area. Segregation of duties reduces the risk of intentional manipulation or error. Where segregation of duties is not feasible, this must be managed through closer supervision. Segregation of duties can be effected through:-

  - **SEPARATION OF DUTIES**

  There should be a well defined division of responsibilities between departments, sections and individuals so that no one person handles a transaction from beginning to end. The duties should be clearly defined in writing, together with the extent (usually in monetary terms) of their respective authorities. There should be a division of responsibilities in respect of each transaction for:-
  - Authorising or initiating the transaction
  - Physical custody and control of the assets related to the transaction
  - Recording of the transaction in the accounting records

  The objective of such a division is principally to detect innocent errors or oversight. Errors are more likely to go undetected if a person checks their own work. The second goal is to ensure that no one person is left in a position to misappropriate an asset and to conceal that action through falsification of the relevant records.

  - **ROTATION OF DUTIES**

  Where practical, arrangements should be made for the duties of employees to be rotated so that no one person deals with one aspect of the organisation's accounting records on a continuous basis.

- **ORGANISATION (PREVENTIVE)**
  The organisation defines and allocates responsibilities and identifies lines of reporting for all aspects of its operations, including controls. The delegation of authority must be appropriate and responsibility will be clearly specified within the overall departmental structure.

- **PHYSICAL (PREVENTIVE)**
  Procedures and security measures will be reviewed on a regular basis at department level, to ensure that access to the cash office is limited to authorised personnel. The appropriateness of controls in place in the case of valuable, portable or desirable assets will also be reviewed.

- **MANAGEMENT (DETECTIVE)**
  Management is responsible for ensuring there are adequate measures to prevent and detect fraud and corruption within the areas under their control.

  Achievement of this is assisted by:-
  - Having processes in place to deter and detect fraud
  - Compliance with Carlow County Council's policies, rules and regulations
  - Ensuring employees understand their responsibilities, through adequate supervision, written procedures and job descriptions
  - Responding positively to recommendations made and advice given by internal and external audit
  - Dealing effectively with issues raised by employees (including taking appropriate action to deal with reported or suspected fraudulent activity)

- **PERSONNEL (PREVENTIVE)**
  Employees must be appropriately qualified and fully trained so as to be competent to carry out the work entrusted to them.

- **SUPERVISION (DETECTIVE AND CORRECTIVE)**
  All areas of operations are subject to checking by supervisory personnel. The level of supervision is relevant to the inherent risk of the activity being supervised. Prescribed procedures for local supervisors will be determined by management at departmental level. Supervision represents the final approval of documents after they have been subjected to the relevant basic controls, but before further processing takes place. Authorisation should not be perceived as being simply a *"rubber stamping"* exercise. It should involve a reasonable degree of scrutiny and control otherwise it serves little purpose. Supervisory controls can only be regarded as effective where the signature of the supervising official exists to evidence the control function that was carried out.

- **ARITHMETIC AND ACCOUNTING (DETECTIVE AND CORRECTIVE)**
  All financial transactions must be approved by an authorised person. It is the responsibility of the authorised person to ensure that transactions are accurately recorded and that proper approvals and processes are in place. Basic Accounting Controls are designed to ensure that the organisation's transactions are valid and that they are recorded completely and accurately in the Council's Financial Management System. Control accounts and reconciliations to the Financial Management System's records are essential elements of good internal control.

- **AUTHORISATION AND APPROVAL (PREVENTIVE)**
  Chief Executive Orders set out the authorisations and approvals for the purchase of goods and services. Adequate authority levels should be established and set out for the initiation or approval of transactions for each individual business area. Actions must be performed by the appropriate personnel (with the right level of seniority/with a Chief Executive's Order if required) and at the right time (before an order is made or a payment generated).

APPENDIX C

CATEGORIES OF RISK

There are six categories of risk which need to be considered and addressed when developing a system of internal controls within any business section:-

1. **FINANCIAL**
2. **OPERATIONAL**
3. **PHYSICAL**
4. **EXTERNAL**
5. **PERSONNEL**
6. **INFORMATION TECHNOLOGY**

1. FINANCIAL

Council activities in this area relate to assets, goods and service procurement procedures, contracts, making payments and the collection of monies. The scale of the risk depends on the amount of money involved and the maintenance and effectiveness of the controls which are in place. Some of the more common financial activities susceptible to fraud are:-

Expenditure	Income
- Purchase/hire of machinery	- Cash handling
- Contract payments	- Fees for services
- Misuse of assets	- Loan repayments
- Insurance claims	- Debt collection
- Goods/services procurement	- Fines

2. OPERATIONAL

The operational activities refer to items such as:-

- Information used for decision making
- Quality of decisions made
- Exploitation of opportunities to make gains
- Reputation of the organisation

3. PHYSICAL

The physical aspect of risk concerns access restrictions to assets such as:-

- Premises
- Plant and machinery
- Cash
- Computers
- Records and documentation

Regular comprehensive stock takes that are reconciled back to Council accounts will act as a powerful deterrent in these areas and re-enforce the Council's strong commitment to fraud prevention.

4. EXTERNAL

These risks are associated with support systems and may involve the misappropriation of plant and machinery. They also include risks associated with outside influences such as suppliers, competing firms, agents, clients and customers.

5. PERSONNEL

Research suggests that the majority of frauds result from the exploitation of an opportunity that presents itself. As a result, it is difficult to generalise about the behaviour of employees and the situations that lead to the possibility of fraud. Managers and supervisors should be ever alert to the potential and/or possibility of fraud in the day to day working environment. They should also be aware of the possibility of collusion both from within and outside the Council in the perpetration of fraud.

Then general tenet of the Council's personnel policy is derived from:-

- Part 15 of the Local Government Act, '01 detailing the Ethical Framework for the Local Government service
- Code of Conduct for Employees, published by the Department in January, '07
- Local Government (Officers) Regulations, 1984, and the Rules of Conduct for Officers of Local Authorities (as amended by the Local Government Act '01)

All new recruits to the Council will be made aware of the existence of this "Fraud Prevention Policy" as part of their induction.

6. INFORMATION TECHNOLOGY FRAUD

It is essential that the ICT Department have policies in place to ensure that the proper controls, practices and procedures exist to protect the Council against computer fraud and ensure that security measures are in place to protect the availability, confidentiality and integrity of IT systems and data.

From falling for phishing emails, clicking on links or downloading documents that turn out to be malware, to being a victim of business email compromise (BEC) scams that end up losing a lot of money, employees are the greatest liability when it comes to cyber security. Educating employees is a key step, but this requires resources and the participation of employees.

Most commonly, unsuspecting staff are compromised by schemes such as email phishing, spoof websites and downloads with embedded malware. By making employees aware of the financial losses associated with cyber attacks, they will take responsibility for their own cyber hygiene.

APPENDIX D

CRIMINAL JUSTICE (CORRUPTION OFFENCES) ACT 2018

The Criminal Justice (Corruption Offences) Act, 2018, commenced on the 30th July, '18. The following summarises some of the substantive changes made in this Act.

- Offences under the Act involve directly and indirectly, corruptly giving or receiving *"a gift, consideration or advantage"* as an inducement or reward for doing an act in relation to office, employment or business or trading in influence.

- Section 7 makes specific provision in relation to Irish officials (set out in Section 2 as including an officer, director, employee or a member of an Irish public body, including a member of a Local Authority) regarding acts in office and use of public information.

- Creating or using a false or misleading document for an improper use is an offence. A *"document"* is broadly defined in the Act to include data held electronically on devices (Section 9).

- Acts outside the State may be offences.

- Presumptions reversing the onus of proof in cases relating to tenders, contracts, grants, loans and licences, land transactions, planning and prosecution of offences and in respect of real and personal property not recorded in statements under the Ethics in Public Office Act, 1995.

- Penalties imposed on Irish officials may include loss of office and may impose a bar on some officials holding a position for up to 10 years.

- Under Section 18, a body corporate shall be guilty of an offence if it is committed not only by a director, manager, secretary or other officer of the body corporate, or a person purporting to act in that capacity, but also by an employee, agent or subsidiary of the body corporate with the intention of obtaining or retaining business for the body corporate, or an advantage in the conduct of business for the body corporate. Where a corporate body has committed an offence, additional convictions can accrue to other complicit managers etc. where an offence is committed by a body corporate and it is proved that the offence was committed with the consent, connivance or wilful neglect of senior officers, that person, as well as the body corporate, shall be guilty of an offence.

- Under Section 18 it will be a defence to a prosecution where the corporate body proves it took all reasonable steps and exercised all due diligence to avoid the commission of the offence. This risk must be evaluated and policies designed and implemented to address any identified risks.