

## **PART 5**

# **CODES AND PROTOCOLS**

## **COUNCILLORS' CODE OF CONDUCT**

The Council, on 15<sup>th</sup> May, 2007 adopted the following Model Code of Conduct promulgated pursuant to the provisions of the Local Government Act, 2000 (as evoked by the Local Authorities (Model Code of Conduct) Order, 2007).

All non-councillor Members of the Standards Committee will be required to observe the Code of Conduct for Councillors.

### **PART 1**

#### **General provisions**

##### **Introduction and interpretation**

- 1. —** (1) This Code applies to **you** as a member of an authority.
- (2) You should read this Code together with the general principles prescribed by the Secretary of State (See Note 1 below).
- (3) It is your responsibility to comply with the provisions of this Code.
- (4) In this Code—
- "meeting" means any meeting of—
- (a) the authority;
- (b) the executive of the authority;
- (c) any of the authority's or its executive's committees, sub-committees, joint committees, joint sub-committees, or area committees;
- "member" includes a co-opted member and an appointed member.
- (5) In relation to a parish council, references to an authority's monitoring officer and an authority's standards committee shall be read, respectively, as references to the monitoring officer and the standards committee of the district council or unitary county council which has functions in relation to the parish council for which it is responsible under section 55(12) of the Local Government Act 2000.

##### **Scope**

- 2. —** (1) Subject to sub-paragraphs (2) to (5), you must comply with this Code whenever you—
- (a) conduct the business of your authority (which, in this Code, includes the business of the office to which you are elected or appointed); or
- (b) act, claim to act or give the impression you are acting as a representative of your authority,

*May, 2011*

and references to your official capacity are construed accordingly.

- (2) Subject to sub-paragraphs (3) and (4), this Code does not have effect in relation to your conduct other than where it is in your official capacity.
- (3) In addition to having effect in relation to conduct in your official capacity, paragraphs 3(2)(c), 5 and 6(a) also have effect, at any other time, where that conduct constitutes a criminal offence for which you have been convicted.
- (4) Conduct to which this Code applies (whether that is conduct in your official capacity or conduct mentioned in sub-paragraph (3)) includes a criminal offence for which you are convicted (including an offence you committed before the date you took office, but for which you are convicted after that date).
- (5) Where you act as a representative of your authority—
  - (a) on another relevant authority, you must, when acting for that other authority, comply with that other authority's code of conduct; or
  - (b) on any other body, you must, when acting for that other body, comply with your authority's code of conduct, except and insofar as it conflicts with any other lawful obligations to which that other body may be subject.

### **General obligations**

- 3. —**
- (1) You must treat others with respect.
  - (2) You must not—
    - (a) do anything which may cause your authority to breach any of the equality enactments (as defined in section 33 of the Equality Act 2006 (See Note 2 below))
    - (b) bully any person;
    - (c) intimidate or attempt to intimidate any person who is or is likely to be—
      - (i) a complainant,
      - (ii) a witness, or
      - (iii) involved in the administration of any investigation or proceedings,in relation to an allegation that a member (including yourself) has failed to comply with his or her authority's code of conduct; or
    - (d) do anything which compromises or is likely to compromise the impartiality of those who work for, or on behalf of, your authority.

**4. —** You must not—

- (a) disclose information given to you in confidence by anyone, or information acquired by you which you believe, or ought reasonably to be aware, is of a confidential nature, except where—
  - (i) you have the consent of a person authorised to give it;
  - (ii) you are required by law to do so;
  - (iii) the disclosure is made to a third party for the purpose of obtaining professional advice provided that the third party agrees not to disclose the information to any other person; or
  - (iv) the disclosure is—
    - (aa) reasonable and in the public interest; and
    - (bb) made in good faith and in compliance with the reasonable requirements of the authority; or
- (b) prevent another person from gaining access to information to which that person is entitled by law.

**5. —** You must not conduct yourself in a manner which could reasonably be regarded as bringing your office or authority into disrepute.

**6. —** You—

- (a) must not use or attempt to use your position as a member improperly to confer on or secure for yourself or any other person, an advantage or disadvantage; and
- (b) must, when using or authorising the use by others of the resources of your authority—
  - (i) act in accordance with your authority's reasonable requirements;
  - (ii) ensure that such resources are not used improperly for political purposes (including party political purposes); and
- (c) must have regard to any applicable Local Authority Code of Publicity made under the Local Government Act 1986.

**7. —** (1) When reaching decisions on any matter you must have regard to any relevant advice provided to you by—

- (a) your authority's chief finance officer; or
- (b) your authority's monitoring officer,

where that officer is acting pursuant to his or her statutory duties.

- (2) You must give reasons for all decisions in accordance with any statutory requirements and any reasonable additional requirements imposed by your authority.

## **PART 2**

### **Interests**

#### **Personal interests**

- 8. —** (1) You have a personal interest in any business of your authority where either—
- (a) it relates to or is likely to affect—
- (i) any body of which you are a member or in a position of general control or management and to which you are appointed or nominated by your authority;
  - (ii) any body—
    - (aa) exercising functions of a public nature;
    - (bb) directed to charitable purposes; or
    - (cc) one of whose principal purposes includes the influence of public opinion or policy (including any political party or trade union),of which you are a member or in a position of general control or management;
  - (iii) any employment or business carried on by you;
  - (iv) any person or body who employs or has appointed you;
  - (v) any person or body, other than a relevant authority, who has made a payment to you in respect of your election or any expenses incurred by you in carrying out your duties;
  - (vi) any person or body who has a place of business or land in your authority's area, and in whom you have a beneficial interest in a class of securities of that person or body that exceeds the nominal value of £25,000 or one hundredth of the total issued share capital (whichever is the lower);
  - (vii) any contract for goods, services or works made between your authority and you or a firm in which you are a partner, a company of which you are a remunerated director, or a person or body of the description specified in paragraph (vi);
  - (viii) the interests of any person from whom you have received a gift or hospitality with an estimated value of at least £25;
  - (ix) any land in your authority's area in which you have a beneficial interest;

- (x) any land where the landlord is your authority and you are, or a firm in which you are a partner, a company of which you are a remunerated director, or a person or body of the description specified in paragraph (vi) is, the tenant;
  - (xi) any land in the authority's area for which you have a licence (alone or jointly with others) to occupy for 28 days or longer; or
- (b) a decision in relation to that business might reasonably be regarded as affecting your well-being or financial position or the well-being or financial position of a relevant person to a greater extent than the majority of—
- (i) (in the case of authorities with electoral divisions or wards) other council tax payers, ratepayers or inhabitants of the electoral division or ward, as the case may be, affected by the decision;
  - (ii) (in the case of the Greater London Authority) other council tax payers, ratepayers or inhabitants of the Assembly constituency affected by the decision; or
  - (iii) (in all other cases) other council tax payers, ratepayers or inhabitants of your authority's area.
- (2) In sub-paragraph (1)(b), a relevant person is—
- (a) a member of your family or any person with whom you have a close association; or
  - (b) any person or body who employs or has appointed such persons, any firm in which they are a partner, or any company of which they are directors;
  - (c) any person or body in whom such persons have a beneficial interest in a class of securities exceeding the nominal value of £25,000; or
  - (d) any body of a type described in sub-paragraph (1)(a)(i) or (ii).

### **Disclosure of personal interests**

- 9. —** (1) Subject to sub-paragraphs (2) to (7), where you have a personal interest in any business of your authority and you attend a meeting of your authority at which the business is considered, you must disclose to that meeting the existence and nature of that interest at the commencement of that consideration, or when the interest becomes apparent.
- (2) Where you have a personal interest in any business of your authority which relates to or is likely to affect a person described in paragraph 8(1)(a)(i) or 8(1)(a)(ii)(aa), you need only disclose to the meeting the existence and nature of that interest when you address the meeting on that business.
- (3) Where you have a personal interest in any business of the authority of the type mentioned in paragraph 8(1)(a)(viii), you need not disclose the

nature or existence of that interest to the meeting if the interest was registered more than three years before the date of the meeting.

- (4) Sub-paragraph (1) only applies where you are aware or ought reasonably to be aware of the existence of the personal interest.
- (5) Where you have a personal interest but, by virtue of paragraph 14, sensitive information relating to it is not registered in your authority's register of members' interests, you must indicate to the meeting that you have a personal interest, but need not disclose the sensitive information to the meeting.
- (6) Subject to paragraph 12(1)(b), where you have a personal interest in any business of your authority and you have made an executive decision in relation to that business, you must ensure that any written statement of that decision records the existence and nature of that interest.
- (7) In this paragraph, "executive decision" is to be construed in accordance with any regulations made by the Secretary of State under section 22 of the Local Government Act 2000.

### **Prejudicial interest generally**

- 10.** — (1) Subject to sub-paragraph (2), where you have a personal interest in any business of your authority you also have a prejudicial interest in that business where the interest is one which a member of the public with knowledge of the relevant facts would reasonably regard as so significant that it is likely to prejudice your judgement of the public interest.
- (2) You do not have a prejudicial interest in any business of the authority where that business—
- (a) does not affect your financial position or the financial position of a person or body described in paragraph 8;
  - (b) does not relate to the determining of any approval, consent, licence, permission or registration in relation to you or any person or body described in paragraph 8; or
  - (c) relates to the functions of your authority in respect of—
    - (i) housing, where you are a tenant of your authority provided that those functions do not relate particularly to your tenancy or lease;
    - (ii) school meals or school transport and travelling expenses, where you are a parent or guardian of a child in full time education, or are a parent governor of a school, unless it relates particularly to the school which the child attends;
    - (iii) statutory sick pay under Part XI of the Social Security Contributions and Benefits Act 1992, where you are in receipt of, or are entitled to the receipt of, such pay;
    - (iv) an allowance, payment or indemnity given to members;
    - (v) any ceremonial honour given to members; and

- (vi) setting council tax or a precept under the Local Government Finance Act 1992.

### **Prejudicial interests arising in relation to overview and scrutiny committees**

- 11.** — You also have a prejudicial interest in any business before an overview and scrutiny committee of your authority (or of a sub-committee of such a committee) where—
- (a) that business relates to a decision made (whether implemented or not) or action taken by your authority's executive or another of your authority's committees, sub-committees, joint committees or joint sub-committees; and
  - (b) at the time the decision was made or action was taken, you were a member of the executive, committee, sub-committee, joint committee or joint sub-committee mentioned in paragraph (a) and you were present when that decision was made or action was taken.

### **Effect of prejudicial interests on participation**

- 12.** — (1) Subject to sub-paragraph (2), where you have a prejudicial interest in any business of your authority—
- (a) you must withdraw from the room or chamber where a meeting considering the business is being held—
    - (i) in a case where sub-paragraph (2) applies, immediately after making representations, answering questions or giving evidence;
    - (ii) in any other case, whenever it becomes apparent that the business is being considered at that meeting;
- unless you have obtained a dispensation from your authority's standards committee;
- (b) you must not exercise executive functions in relation to that business; and
  - (c) you must not seek improperly to influence a decision about that business.
- (2) Where you have a prejudicial interest in any business of your authority, you may attend a meeting (including a meeting of the overview and scrutiny committee of your authority or of a sub-committee of such a committee) but only for the purpose of making representations, answering questions or giving evidence relating to the business, provided that the public are also allowed to attend the meeting for the same purpose, whether under a statutory right or otherwise.

### Part 3

#### Registration of Members' Interests

##### Registration of members' interests

- 13.** — (1) Subject to paragraph 14, you must, within 28 days of—
- (a) this Code being adopted by or applied to your authority; or
  - (b) your election or appointment to office (where that is later),
- register in your authority's register of members' interests (maintained under section 81(1) of the Local Government Act 2000) details of your personal interests where they fall within a category mentioned in paragraph 8(1)(a), by providing written notification to your authority's monitoring officer.
- (2) Subject to paragraph 14, you must, within 28 days of becoming aware of any new personal interest or change to any personal interest registered under paragraph (1), register details of that new personal interest or change by providing written notification to your authority's monitoring officer.

##### Sensitive information

- 14.** — (1) Where you consider that the information relating to any of your personal interests is sensitive information, and your authority's monitoring officer agrees, you need not include that information when registering that interest, or, as the case may be, a change to that interest under paragraph 13.
- (2) You must, within 28 days of becoming aware of any change of circumstances which means that information excluded under paragraph (1) is no longer sensitive information, notify your authority's monitoring officer asking that the information be included in your authority's register of members' interests.
- (3) In this Code, "sensitive information" means information whose availability for inspection by the public creates, or is likely to create, a serious risk that you or a person who lives with you may be subjected to violence or intimidation.

## **NOTES**

(NB. These notes do not constitute Part of the Code of Conduct)

### **Note 1 — Extract from the Relevant Authorities (General Principles) Order, 2001**

#### THE GENERAL PRINCIPLES

##### *Selflessness*

1. Members should serve only the public interest and should never improperly confer an advantage or disadvantage on any person.

##### *Honesty and Integrity*

2. Members should not place themselves in situations where their honesty and integrity may be questioned, should not behave improperly and should on all occasions avoid the appearance of such behaviour.

##### *Objectivity*

3. Members should make decisions on merit, including when making appointments, awarding contracts, or recommending individuals for rewards or benefits.

##### *Accountability*

4. Members should be accountable to the public for their actions and the manner in which they carry out their responsibilities, and should co-operate fully and honestly with any scrutiny appropriate to their particular office.

##### *Openness*

5. Members should be as open as possible about their actions and those of their authority, and should be prepared to give reasons for those actions.

##### *Personal Judgement*

6. Members may take account of the views of others, including their political groups, but should reach their own conclusions on the issues before them and act in accordance with those conclusions.

##### *Respect for Others*

7. Members should promote equality by not discriminating unlawfully against any person, and by treating people with respect, regardless of their race, age, religion, gender, sexual orientation or disability. They should respect the impartiality and integrity of the authority's statutory officers, and its other employees.

##### *Duty to Uphold the Law*

8. Members should uphold the law and, on all occasions, act in accordance with the trust that the public is entitled to place in them.

May, 2011

### *Stewardship*

9. Members should do whatever they are able to do to ensure that their authorities use their resources prudently and in accordance with the law.

### *Leadership*

10. Members should promote and support these principles by leadership, and by example, and should act in a way that secures or preserves public confidence.

## **NOTE 2 – Equalities Act, 2006: Section 33**

### **33. Equality and Human Rights Enactments**

- (1) In this Part "the equality enactments" means—
  - (a) the Equal pay Act, 1970 (c.41)
  - (b) the Sex Discrimination Act, 1975
  - (c) the Race Relations Act, 1976,
  - (d) the Disability Discrimination Act, 1995
  - (e) Part 2 of this Act
  - (f) Regulations under Part 3 of this Act
  - (g) the Employment Equality (Sexual Orientation) Regulations 2003 (S.I. 2003/1661), and
  - (h) the Employment Equality (Religion or Belief) Regulations 2003 (S.I. 2003/1660)
- (2) In this Part "the equality and human rights enactments" means the equality enactments and the Human Rights Act, 1998 (c.42)
- (3) The Secretary of State may by order amend the list in subsection (1) so as to:
  - (a) add an entry;
  - (b) remove an entry, or
  - (c) vary an entry.

# **EMPLOYEES'**

# **CODE OF CONDUCT**

## **EMPLOYEES' CODE OF CONDUCT**

**Note: Throughout this section references to the Head of Paid Service, Chief Finance Officer, Monitoring Officer, Strategic Management Team, Directors, Heads of Service and Service Managers should be construed with reference to definitions in Article 12 of this Constitution.**

### **1. BUSINESS, PRIVATE WORK AND GIFTS**

It is not acceptable for staff to undertake private work that may give rise to a conflict between the duties of the council and their duties to a private individual or organisation. Staff should not become involved in a private capacity in any way whatsoever in any matter on which the Council has to make a decision, e.g. Planning and Building Regulation Applications, or any matter in which the Council are involved, e.g. legal work, Grant Applications, Appeals, etc. The public and Members of the Council are entitled to expect their Officers to be entirely independent in such matters and any Officer who undertakes private work in breach of this instruction, without written authority from the appropriate Member of the Strategic Management/Head of Service, will be guilty of Gross Misconduct and will be dismissed.

Notwithstanding the policy, in exceptional cases, the Council may be prepared to give consent for an Officer to undertake work of this nature and applications for consent, giving a detailed justification, should be submitted in writing to the appropriate member of the Strategic Management Team/Head of Service. Any difficulties of interpretation should also be referred to the appropriate Member of the Strategic Management Team/Head of Service.

For confirmation on a particular matter please read the following guidelines.

### **2. GUIDELINES RELATING TO CONDUCT OF EMPLOYEES**

#### **2.1 Introduction**

2.1.1 These guidelines are intended to assist employees in providing standards of conduct expected by South Staffordshire Council.

2.1.2 They apply to all employees of the Council, irrespective of the particular scheme of conditions the person is employed under.

2.1.3 The guidelines supplement: -

- (i) current legislation, the Local Government Act 1972, (section 117 is included at Appendix 'A'); and
- (ii) the relevant code of Official Conduct as contained in the National Scheme of Conditions of Service relating to the NJC for Local Government Services, JNC for Chief Officers and the JNC for Chief Executives.

2.1.4 The guidelines are intended to offer assistance to all employees and cover the following matters: -

- Declaration of interest
- Other Employment and Payment for Services

*May, 2011*

- Acceptance of Gifts or Hospitality
- Sponsorship of Major Council Events or Activities
- Confidentiality and Accuracy of Information
- Use of Council Facilities and Resources
- Political Interest/Activity
- Discrimination and Equal Opportunities

## **2.2 Declaration of Interest**

2.2.1 Upon the commencement of employment with the Council, all employees are required to “declare their interest” in any matters affecting the decisions and/or operations of the Council. In addition, a declaration should also be made in respect of any subsequent acquisition of an interest. An “interest” should be declared so far as it is known where it involves the following:-

- The employee
- The employee’s spouse or partner
- The employee’s close relatives, ie parent, brother, sister or child.

It is only necessary to disclose an interest where the employee can exert influence on any decision making process.

2.2.2 The declaration should be made in writing and submitted to the appropriate member of the Strategic Management Team/Head of Service who will forward it to the Chief Executive. A central register of interests will be maintained by the Chief Executive and a note of the declaration will be made on the individual’s file.

2.2.3 Employees are reminded of the NJC Scheme of Conditions for Local Government Services that states "Employees will maintain conduct of the highest standard such that public confidence in their integrity is sustained."

## **2.3 Other Employment and Payment for Services**

2.3.1 Before engaging in any business activity or private work, whether paid or unpaid, employees must receive the consent of the appropriate Strategic Management Team/Head of Service. This will allow a decision to be made as to whether such employment or business activity conflicts with the Authority’s interest or in any way weakens public confidence in the Authority’s business. Notification of any business activity or private work must be given in writing.

2.3.2 The Strategic Management Team and the Heads of Service are authorised to give consent provided the activity or work:-

- will not interfere with the employee’s official duties;
- does not generate a conflict of interest with Council business;
- does not relate in any way to the granting of planning permission or building regulation approval within the District, or to other decisions made by the Council or its officers (e.g. purchasing, improvement grants, mortgages); and
- does not in any way relate to contracts entered into by the Council.

2.3.3 The Members of the Strategic Management Team/Head of Service will give any consent in writing and will notify the Chief Executive so that a note

can be retained on the individual's file in the Human Resources Service and a copy retained on a central register maintained by the Chief Executive.

- 2.3.4 Where consent of a member of the Strategic Management Team/ Head of Service is withheld, the employee concerned will have the right of appeal in the first instance to the Chief Executive and then through normal grievance procedures.
- 2.3.5 Where a business activity or form of private work is of a continuous nature, it shall be sufficient for the employee concerned to obtain one consent, provided that any change in the situation is notified by the employee at the earliest opportunity.
- 2.3.6 Where consent is given, the employee must ensure that it is made clear to all concerned that the activity has nothing to do with the Council and no liability rests with the Council. On no account must the activity be carried out during working hours and none of the Council's equipment or facilities should be used. In particular, telephone calls should not be taken at the offices of the Council and the Council's telephone number should not be given to third parties.
- 2.3.7 In the event that a fee is paid in respect of the provision of a service carried out by an individual in their capacity as an Employee of the Council, the fee should be made payable to the Council and not to the Officer concerned.
- 2.3.8 A register of other employment and payment for services will be maintained by the Chief Executive.
- 2.3.9 Employees are reminded of the relevant Scheme of Conditions relating to Official Conduct.

## **2.4 Acceptance of Gifts**

- 2.4.1 The acceptance of gifts by employees in their individual capacity could be viewed with suspicion by members of the public and make the employee and the Council vulnerable to criticism. Consequently, as a general rule, employees should tactfully refuse offers of gifts.
- 2.4.2 Modest gifts of a promotional nature, given by way of trade advertisements to a wide range of people, are acceptable. These include calendars, diaries, tape measures and articles for office use, e.g. pens, ashtrays. Also acceptable are gifts, whether or not of a promotional nature, offered at the conclusion of a courtesy visit to a factory or other premises. It is considered that a modest gift would not exceed the value of £25.00 and receipt of any gift valued higher than this must be notified to the Chief Executive.
- 2.4.3 If an employee receives a significant gift i.e. of a value estimated at over £25.00 without warning (for example, via the post), the employee should immediately inform the appropriate member of the Strategic Management Team/Head of Service of this matter. The appropriate member of the Strategic Management/Head of Service will then become responsible, in consultation with the Chief Executive, in deciding upon the appropriate action to be taken. This action may involve the return of the gift to the

sender or forwarding it on to some charitable or deserving cause, or other measures. The member of the Strategic Management Team/Head of Service concerned should inform the donor, in writing, of the action taken.

- 2.4.4 There may be occasions where it is not possible to refuse a significant gift without giving offence or where it would be churlish to refuse. In such cases the employee should immediately inform the appropriate member of the Strategic Management Team/Head of Service and enter receipt of the gift in the central register held by the Monitoring Officer.
- 2.4.5 In summary, if there is any doubt about whether a gift may be accepted, the gift should be politely and tactfully refused.

## **2.5 Offers and Acceptance of Hospitality**

- 2.5.1 Whether employees should accept hospitality as a result of their employment at the Council is very much a matter of judgement given the particular circumstances. It must be apparent that no cause could reasonably arise for adverse criticism of the Council or individuals following the acceptance of any hospitality. It is important that any suggestion of improper influence is completely avoided. In such instances where any suggestion of improper influence is even remotely possible, the offer of hospitality must be politely refused by the employee.
- 2.5.2 The following hospitality would generally be considered acceptable:-
- (a) An offer of a drink following a site visit.
  - (b) Hospitality offered by other non-commercial or charitable bodies, provided that there is a general understanding that no indebtedness will result from the acceptance.
  - (c) Invitations to functions the employee represents the Council in an official capacity, for example, when invited to speak, opening ceremonies, trade shows.
  - (d) Invitations to functions where attendance would be by virtue of the employee's position and as a representative of the Council.
  - (e) A working lunch where acceptance does not put the individual's personal integrity, or that of the Council, into question.
  - (f) Hospitality of the "corporate entertaining" nature, for example, at sports, social or training events, or at conferences (where others are being simultaneously entertained), is acceptable if there is a general understanding that no indebtedness will result from acceptance. Unless specifically authorised as a duty, the employee would be expected to take leave if it occurs during working time.
- 2.5.3 Offers of hospitality that appear immodest or lavish should be refused and the offer reported to the appropriate member of the Strategic Management Team/Head of Service or to the Chief Executive.
- 2.5.4 Prior to accepting any offer of hospitality, the views of the appropriate member of the Strategic Management Team/ Head of Service or Chief Executive should be sought. Receipt of any hospitality should be entered in the central register held by the Monitoring Officer.

## **2.6 Sponsorship of Major Council Events, Activities or Publications**

2.6.1 All offers of sponsorship should be notified to the Chief Executive. Any sponsorship with a value greater than £500 requires the approval of the Chief Executive.

2.6.2 The record of sponsorship will include: -

- (a) Name of sponsor and type of sponsorship offered; and
- (b) Approval or refusal of the Chief Executive, where appropriate.

Details are to be notified on the relevant form and forwarded to the Chief Executive for retention on the Central Register of Sponsorship.

## **2.7 Confidentiality and Accuracy of Information**

2.7.1 The confidentiality of information received in the course of an employee's duty should be respected and should never be used for personal or political gain.

2.7.2 No employee shall communicate to the public the proceedings of any confidential section of the Council's meetings, etc. nor the contents of any document relating to the Council unless required to do so by law or expressly authorised to do so by the appropriate member of the Strategic Management Team/Head of Service. Confidentiality remains when the employee has left the employment of the Council.

2.7.3 Information given by an employee in the course of a duty should be true and fair and never designed to mislead.

## **2.8 Use of Council Facilities, Resources, etc**

2.8.1 Any facilities, equipment, tools, etc. provided by the Council for use in an employee's duties should be used only for those duties and for no other purpose except where prior approval has been granted by the appropriate Member of the Strategic Management Team/Head of Service. This applies to all facilities and property, including use of telephones, photocopiers, vehicles or other similar equipment.

2.8.2 Where arrangements are in place for employees to make payment for the private use of equipment, such as telephone calls and photocopiers, their position of trust should not be abused. It should be noted this does not give employees the right to use these "paid for" services to the extent that such use interferes with the duties of their post. In particular, telephone calls should be restricted to urgent or emergency use only and the Council's telephone numbers should not be given to third parties.

2.8.3 No employees should use their position to gain the use of Council or other services without payment of the appropriate charges. The approved arrangements for the use of equipment, services, etc for private use should always be followed.

## **2.9 Political Interest/Activity**

- 2.9.1 Employees are reminded of their political neutrality and that they serve the Council as a whole and must ensure that the individual rights of members are respected.
- 2.9.2 It is vital that both the Council and the public are confident that employees will serve loyally and impartially. It is essential that in fulfilling their duties and responsibilities employee's own political views do not influence decisions or recommendations.
- 2.9.3 Employees should not carry out any political activity which in any way might confuse the public about whether or not they are still acting as a Council employee.
- 2.9.4 Certain posts are designated as "politically restricted" and have additional conditions laid on them. These posts will have been identified and details issued previously, should there remain any uncertainty employees should contact Human Resources for advice.

## **2.10 Discrimination and Equal Opportunities**

- 2.10.1 The Council is an equal opportunity employer and does not discriminate unlawfully in employment practices nor in the provision of facilities and services to the public by reference to sex, marital status, race, religion or belief, age, or disability. Employees should avoid direct and indirect discrimination in all matters relating to the public and fellow employees.

## **2.11 Failure to comply**

- 2.11.1 The conduct of all employees should be such that they remain immune from any criticism or suspicion that their actions or decisions have been unduly influenced. Employees are expected to use common sense in assessing any situation where this could be construed. No employees should act in any manner that could give rise to such accusations.
- 2.11.2 It is the responsibility of every employee to maintain the standards and integrity expected in public service. It is also each employee's responsibility to bring to the attention of the appropriate member of the Strategic Management Team/Head of Service any deficiency in the provision of that service and report any impropriety or breach of procedure.
- 2.11.3 Any employee failing to comply with this code of conduct will be liable to disciplinary action which may result in their dismissal.

**Guidelines relating to Conduct of Officers**

**Local Government Act 1972 – Extract**

**Section 117**

117-(1) If it comes to the knowledge of an officer employed, whether under this Act or any other enactment, by a local authority that a contract in which he has any pecuniary interest, whether direct or indirect (not being a contract to which he is himself a party), has been, or is proposed to be, entered into by the authority or any committee thereof, he shall as soon as practicable give notice in writing to the authority of the fact that he is interested therein.

For the purposes of this section an Officer shall be treated as having indirectly a pecuniary interest in a contract or proposed contract if he would have been so treated by virtue of section 95 above had he been a member of the authority.

- (2) An officer of a local authority shall not, under colour of his office or employment, accept any fee or reward whatsoever other than his proper remuneration.
- (3) Any person who contravenes the provisions of subsection (1) or (2) above shall be liable on summary conviction to a fine not exceeding (Level 4 on the standard scale).



# **PROTOCOL ON COUNCILLOR/EMPLOYEE RELATIONS**

## **PROTOCOL ON COUNCILLOR/EMPLOYEE RELATIONS**

**Note: Note: Throughout this section references to the Head of Paid Service, Chief Finance Officer, Monitoring Officer, Strategic Management Team, Directors, Heads of Service and Service Managers should be construed with reference to definitions in Article 12 of this Constitution.**

### **1. INTRODUCTION**

- 1.1 The relationship between councillors and employees is an essential ingredient that goes into the successful working of the organisation. This relationship within South Staffordshire Council is characterised by mutual respect, informality and trust. Councillors and employees feel free to speak to one another openly and honestly. Nothing in this Protocol is intended to change this relationship. The purpose of this Protocol is rather to help councillors and employees to perform effectively by giving guidance on their respective roles and expectations and on their relationship with each other. The Protocol also gives guidance on what to do on the rare occasions when things go wrong. Responsibility for the operation of this Protocol lies with the Human Resources Manager.
- 1.2 The Protocol must be read and operated in the context of any relevant legislation and national and local Codes of Conduct and any procedure for confidential reporting.

### **2. ROLES OF COUNCILLORS AND EMPLOYEES**

- 2.1 The respective roles of councillors and employees can be summarised as follows:

Councillors and employees are servants of the public and they are indispensable to one another. But their responsibilities are distinct. Councillors are responsible to the electorate and serve only so long as their term of office lasts. Employees are responsible to the Council. Their job is to give advice to Councillors and the Council, and to carry out the Council's work under the direction and control of the Council, the Executive, and relevant committees, panels, etc.

Mutual respect between Councillors and employees is essential to good local government.

- 2.2 Councillors

Councillors have three main areas of responsibility: determining the policy of the Council and giving it political Leadership, representing the Council externally, and acting as advocates on behalf of their constituents. It is not the role of members to involve themselves in the day to day management of Council services.

- 2.3 Members of the Executive, Chairmen of Committees

Members of the Executive and Chairmen of Committees, Panels etc have additional responsibilities. Because of those responsibilities, their relationships with employees may be different from, and more complex than those of councillors without those responsibilities, and this is recognised in the expectations they are entitled to have.

*May, 2011*

## 2.4 Opposition Members

As individual members of the Council, all councillors have the same rights and obligations in their relationship with employees and should be treated equally. This principle is particularly important in the context of scrutiny and overview. However, where a political group forms an administration, either alone or in partnership with another group or groups, it is recognised that the relationship between employees, particularly those at a senior level in the organisation, and the administration will differ from that with opposition groups.

## 2.5 Employees

The role of employees is to give advice and information to members and to implement the policies determined by the Council.

Certain employees e.g. Head of Paid Service, Monitoring Officer and Chief Finance Officer (Section 151 Officer) have responsibilities in law over and above their obligations to the Council and its Members that they must be allowed to discharge.

## **3. EXPECTATIONS**

Councillors can expect from employees:

- A commitment to the Council as a whole, and not to any political group
- A working partnership
- An understanding of and support for respective roles, workloads and pressures
- Timely response to enquiries and complaints
- Professional advice, not influenced by political views or preference, which does not compromise the political neutrality of employees.
- Regular, up to date information on matters that can reasonably be considered appropriate and relevant to their needs, having regard to any individual responsibilities that they have and positions that they hold
- Awareness of and sensitivity to the political environment
- Respect, dignity and courtesy
- Training and development in order to carry out their role effectively
- Integrity, mutual support and appropriate confidentiality
- Not to have personal issues raised with them by employees outside the agreed procedures
- That employees will not use their relationship with members to advance their personal interests or to influence decisions improperly
- That employees will at all times comply with the relevant Code of Conduct

Employees can expect from councillors:

- A working partnership

- An understanding of and support for respective roles, workloads and pressures
- Political Leadership and direction
- Respect, dignity and courtesy
- Integrity, mutual support and appropriate confidentiality
- Not to be subject to bullying or to be put under undue pressure. Members should have regard to the seniority of employees in determining what are reasonable requests, having regard to the power relationship between members and employees, particularly at junior levels
- That councillors will not use their position or relationship with employees to advance their personal interests or those of others or to influence decisions improperly
- That councillors will at all times comply with the relevant Code of Conduct

#### **4. WHEN THINGS GO WRONG**

##### **Procedure for employees**

- 4.1 From time to time the relationship between councillors and employees may break down or become strained. Whilst it will always be preferable to resolve matters informally, through conciliation by an appropriate senior manager or councillor, employees will have recourse to the Harassment and Grievance Procedures or to the Council's Monitoring Officer, as appropriate to the circumstances. In the event of a grievance or complaint being upheld, the matter will be referred to the Chief Executive, who, having advised the Leader of the Council and the appropriate Group Leader will decide on the course of action to be taken, following consultation with the Chairman and Vice Chairman of the Standards Committee.

##### **Procedure for Councillors**

- 4.2 In the event that a councillor is dissatisfied with the conduct, behaviour or performance of an employee, the matter should be raised with the appropriate member of Strategic Management Team (SMT) or Head of Service. Where the employee concerned is a member of SMT or Head of Service, the matter should be raised with the Chief Executive. Where the employee concerned is the Chief Executive, the matter should be raised with the Human Resources Manager. If the matter cannot be resolved informally, it may be necessary to invoke the Council's relevant Disciplinary Procedure.



**South  
Staffordshire  
Council**

**ANTI FRAUD**

**AND**

**CORRUPTION POLICY**

**SOUTH STAFFORDSHIRE COUNCIL**  
**ANTI FRAUD AND CORRUPTION POLICY**

**CONTENTS**

- 1.0 FOREWARD
- 2.0 INTRODUCTION
- 3.0 CORPORATE FRAMEWORK AND CULTURE
- 4.0 PREVENTION
- 5.0 DETECTION AND INVESTIGATION
- 6.0 DETERRENCE
- 7.0 RAISING FRAUD AWARENESS
- 8.0 CONCLUSIONS

Appendix 1 - FRAUD and CORRUPTION RESPONSE PROCEDURE

*September, 2011*

**SOUTH STAFFORDSHIRE COUNCIL**  
**MANAGING the RISK of FRAUD**  
**ANTI-FRAUD AND CORRUPTION POLICY**

**1. Foreword**

- 1.1 The United Kingdom public sector maintains high standards of probity and has a good reputation for protecting the public purse. Sound systems of public accountability are vital to effective management and in maintaining public confidence. The Council shares these high standards and is committed to protecting the public funds entrusted to it. Although we have good policies and procedures they are often ignored: much of our fraud happens when non-compliance with procedures leads to simple checks being neglected. The minimisation of losses to fraud and corruption is essential to ensure that resources are used for their intended purpose to provide services to the residents of South Staffordshire.
- 1.2 The public is entitled to expect the Council to conduct its affairs with integrity, honesty and openness, and to demand the highest standards of conduct from those working for it. This Anti Fraud and Corruption Policy outlines the Council's commitment to creating an anti-fraud culture, and maintaining high ethical standards in its administration of public funds. It also recognises its responsibilities under the various legislation including the Proceeds of Crime Act 2002 and Fraud Act 2006, **Bribery Act 2010** and subsequent regulations.
- 1.3 The Policy is based on a series of comprehensive and inter-related procedures, designed to prevent, detect and deter fraud and to take effective action against any attempted or actual fraudulent act affecting the Council. The Policy also satisfies the legislative requirements to have effective arrangements for tackling fraud, and conforms with professional guidance laid down in the Chartered Institute of Public Finance and Accountancy (CIPFA) Code of Practice for Internal Audit in Local Government.

**2. Introduction**

- 2.1 South Staffordshire's Internal Audit Section, in delivering the Internal Audit function to the Council has the key function of monitoring the effectiveness of internal controls in operation. This also includes carrying out investigations into suspected cases of fraud or corruption. Fraud and corruption can be reported in a number of different ways, which are outlined in sections 3.10 to 3.13 and the Fraud and Corruption Response Procedure (Appendix 1).
- 2.2 The purpose of this Policy is to outline the Council's approach, as well as defining roles and responsibilities, for dealing with the threat of fraud and corruption, both internally and externally. It applies to:
- councillors
  - employees
  - agency staff
  - contractors
  - consultants
  - suppliers

*September, 2011*

- service users
- staff and committee members of organisations funded by the District Council
- staff and principals of partner organisations

In addition to the above, the Council also expects the residents of South Staffordshire to be honest in their dealings with the Council.

- 2.3 This Policy sets out the Council's commitment to tackling fraud and corruption. This makes it clear to all concerned that appropriate and decisive action will be taken against those committing or attempting to commit, fraudulent or corrupt acts against the Council.
- 2.4 In order for the Council to be effective in its approach to dealing with the problem of fraud and corruption it has to set about ensuring that it creates a culture of intolerance rather than indifference to such matters.
- 2.5 The Council's Members and Staff play an important part in creating and maintaining this culture. They are encouraged to raise any matters that concern them relating to the Council's methods of operation, in accordance with the Council's Confidential Reporting ("Whistle Blowing") Policy.

### **3. Corporate Framework and Culture**

- 3.1 The prevention and detection of fraud and corruption and the protection of the public purse is everyone's responsibility
- 3.2 The Council has a range of interrelated policies and procedures that provide a corporate framework to counter fraudulent activity. These have been formulated in line with appropriate legislative requirements, and include:
- Codes of Conduct for members and officers
  - Scheme of Delegation
  - Council Procedure Rules and Financial Regulations
  - Accounting procedures and records
  - Sound internal control systems
  - Effective internal audit, provided by South Staffordshire's Internal Audit Section
  - Effective recruitment and selection procedures
  - Disciplinary Procedure
  - Fraud and Corruption Response Procedure
  - Anti Fraud Framework for the Benefits Section
  - Whistle Blowing Policy
  - The Regulation of Investigatory Powers Act (RIPA) Policy
  - Data Matching Policy
  - Training
  - Any Professional Codes of Ethics
- 3.3 The Council believes that a culture of honesty and openness is a key element in tackling fraud. The Codes of Conduct for Members and Staff are based on the Nolan Principles of Standards in Public Life. Where Members or Staff fail to adhere to these codes appropriate action will be taken against them.
- 3.4 The Fraud Act of 2006 gives us a legislative definition of fraud as the intention to make gain or cause loss by false representation, failing to disclose information or abuse of position. For details of a definition, please see page 17.

*September, 2011*

- 3.5 ***The Bribery Act of 2010 gives us a legislative definition of bribery as "as the giving or taking of a reward in return for acting dishonestly and/or in breach of the law. The reward could relate to money, payment in kind, goods or services".***
- 3.6 The Council is committed to driving down Benefit Fraud. Both public perception and organisational culture play key roles in achieving this aim.
- 3.7 All Members and Staff are therefore required to report any known material changes affecting Benefit claims to the Benefits Section. This specifically includes your own entitlement and of any tenants or sub-tenants that you may have. Failure to do so is an offence under the Social Security Admin (Fraud) Act 2001.
- 3.8 In general terms, this requirement includes the timely transfer of information you receive in your normal business activities relating to any other customer who has alerted you to a fact that affects Benefit awards.
- 3.9 Staff, particularly Benefit Staff, should be required to declare any interest in a Benefit Claim, for example, a relative's claim to benefit, and these cases should be treated "in confidence". The files should be kept separately and assessed by a supervisor to minimise the potential for internal fraud or collusion.
- 3.10 Concerns can be raised knowing they will be treated seriously and properly investigated in a confidential and impartial manner. In raising concerns Staff can be assured that there will be no victimisation, and anonymity will be respected wherever possible. It will not affect their employment situation or future prospects with the Council.
- 3.11 Staff should raise their concerns with the Internal Audit Manager, or in his/her absence, with a member of the Internal Audit Team. Where staff feel unable to raise concerns with the Internal Audit Manager, they can raise their concern with their line manager, who must immediately inform the Internal Audit Manager. Under no circumstances should any investigations be undertaken by any other member of staff.
- 3.12 In addition, a confidential fraud hotline (01902 696252) has been set up for staff and members of the public to report any concerns. Anyone using this facility should provide as much information as possible to ensure the concern can be properly investigated, including leaving your name and contact number, if possible. Concerns made anonymously are much less powerful, but they will be considered in an appropriate manner.
- 3.13 Members of the public and/or staff can also use the generic e-mail address [internal.fraud@sstaffs.gov.uk](mailto:internal.fraud@sstaffs.gov.uk), which is accessed only by internal audit staff.
- 3.14 For housing benefit fraud issues, concerns should be raised with the Benefit Fraud Team or by contacting the Benefit Fraud hotline on 0500 658 008.
- 3.15 Elected Members, suppliers, contractors, and the general public are also encouraged to report concerns through the above routes.
- 3.16 Unless there are good reasons to the contrary, any allegations received by way of confidential letters or telephone calls will be taken seriously and investigated in an appropriate manner. All allegations received in this manner should immediately be forwarded to the Internal Audit Manager.

*September, 2011*

3.17 The investigating Officer will usually be the Audit Manager or another Auditor authorised to do this by the Audit Manager. The investigating Officer will:

- inform the Section 151 Officer (Chief Financial Officer) and Chief Executive, as necessary;
- deal promptly and confidentially with the matter;
- record all evidence received;
- ensure that evidence is sound and adequately supported;
- ensure security of all evidence collected;
- liaise as necessary and appropriate with the relevant Director;
- liaise as necessary with external agencies e.g. Police;
- notify the Council's Insurance Officer, if appropriate; and,
- implement Council disciplinary procedures where appropriate.

A Benefit Investigations Officer will investigate matters concerning National and Local benefits. The Benefit Investigation Team has its own set of procedures, which will be followed.

3.18 The Council will deal swiftly and thoroughly with any member of Staff who attempts to defraud the Council or who is corrupt.

3.19 There is a need to ensure that any investigation process is not misused and, therefore, any abuse such as raising unfounded malicious allegations may be dealt with as a disciplinary matter.

3.20 When it is found that fraud or corruption has occurred due to a break down in the Council's systems or procedures, the relevant members of staff will ensure that appropriate improvements in systems of control are implemented in order to prevent a reoccurrence. Advice will be provided by Internal Audit.

3.21 Formal reports will be issued aimed at addressing control weaknesses and these will be reported to the Audit Committee in the Audit Manager's quarterly progress report.

#### **4. Prevention**

4. The Council recognises that fraud and corruption are costly, both in terms of risk to reputation and financial losses. The prevention of fraud is therefore a key objective of the Council and respective roles and responsibilities are outlined below.

##### **4.1 Employees of the Council**

4.1.1 The Council recognises that staff are often the first line of defence in preventing fraud. A key preventative measure in that fight is the effective recruitment of staff.

4.1.2 Staff recruitment will be undertaken in accordance with the Council's policies for Recruitment and Selection. Written references should be obtained by Human Resources regarding the known honesty and integrity of potential members of staff, and evidence of formal qualifications obtained, before formal employment offers are made. In this regard temporary staff should be treated in the same manner as permanent.

4.1.3 Heads of Service/Service Managers are responsible for ensuring agencies engaged for the supply of temporary Staff have rigorous vetting processes and

*September, 2011*

that references are sought direct from previous clients with regard to the suitability and integrity of the candidate.

- 4.1.4 For certain posts, the Council will undertake additional checks on potential new employees, for example, Criminal Records Bureau checks.
- 4.1.5 All staff must abide by the Council's Code of Conduct for Employees, which sets out requirements on personal conduct. All staff are expected to follow the codes of conduct laid down by their respective professional institutes.
- 4.1.6 Financial Regulations place responsibility for fraud prevention on all employees. Staff should therefore be alert and alerted to the possibility of fraud and to report any concerns. The Council has a confidential reporting 'Whistle Blowing Policy' in place to assist employees in reporting concerns about fraud and other issues without fear of reprisal. The Whistle Blowing Policy can be found on the Council's Intranet.
- 4.1.7 The Council has in place disciplinary procedures for all employees. Those found to have breached the Code of Conduct will be dealt with in accordance with these procedures. Where criminal activity is suspected or found, the matter will be referred to the police for investigation and possible prosecution, in accordance with the Fraud and Corruption Response Procedure. In addition, restitution will be sought from those who are found to have perpetrated fraudulent acts.
- 4.1.8 Staff are reminded that they must operate within Section 117 of the Local Government Act 1972, regarding the disclosure of pecuniary interests in contracts relating to the Council, or the non-acceptance of any fees, gifts, hospitality or any other rewards, other than their proper remuneration. These requirements are set out in the Council's Code of Conduct for Employees.
- 4.1.9 All Staff are required to declare in a public register any offers of gifts (exceeding £25) or hospitality, which are in any way related to the performance of their duties in relation to the Council.
- 4.1.10 Employees should also declare private work etc., which if permitted must be carried out during hours when not employed on Council work, and should not be conducted from Council premises. A record is maintained by the Chief Executive.
- 4.1.11 Staff attention is drawn to the relevant Sections in the disciplinary procedures, which form part of the contract of employment, and Financial Regulations.
- 4.1.12 Management at all levels are responsible for ensuring that their Staff are aware of the Authority's Financial Regulations and Standing Orders, and that the requirements of each are being met. They are also responsible for ensuring that appropriate procedures are in place to safeguard the resources for which they are responsible.
- 4.1.13 Managers should strive to create an environment in which their Staff feel able to approach them with concerns they may have about suspected irregularities. If Managers and Staff are unsure of the appropriate action to take, they should contact the Internal Audit Section.

## 4.2 Council Members

- 4.2.1 Members are required to operate within:

*September, 2011*

- National Code of Local Government Conduct
- Code of Conduct for Members
- Constitution of the Council
- Relevant legislation

- 4.2.2 These matters and other guidance are specifically brought to the attention of members at the induction course for new members and are in each member's handbook. They include rules on the declaration and registration with the Monitoring Officer of potential areas of conflict between members' Council duties and responsibilities, and any other areas of their personal or professional lives.
- 4.2.3 Members are required to provide specific information concerning their financial and other interests and keep this information up to date. The Member's Financial and Other Interests Register is held by the Council's Monitoring Officer.
- 4.2.4 Adherence to these matters is overseen by the Council's Standards Committee, which is responsible for the ethical framework of the Council, working closely with the Monitoring Officer.
- 4.2.5 The Council has established a Standards Committee, which has independent representatives within its membership.
- 4.2.6 The Standards Committee is responsible for:
- promoting high standards of conduct by Councillors (including Parish Councillors);
  - advising the Council and the Parish Councils on the adoption or revision of their Code of Conduct;
  - advising on training for Councillors, Parish Councillors and co-opted members on matters relating to the Code of Conduct;
  - functions relating to standards of conduct of councillors under any relevant provision of or regulations made under Local Government Act 2000, or the Local Government and Public Involvement in Health act 2007;
  - considering any reports from a case tribunal or interim case tribunal and any report from the Standards Board for England/Monitoring Officer or any other matter referred to the Committee pursuant to the Standards Committee (England) Regulations 2008 (and making determinations thereon);
  - determination of applications from District and Parish councillors for dispensation pursuant to the Local Government Act 2000 and the Relevant Authorities (Standards Committee) (Dispensations) Regulations 2002;
  - advising the Council on its Code of Corporate Governance and Ethical Governance Framework;
  - monitoring and advising the Council on its Policy re. Operations carried out under the Regulation of Investigatory Powers Act 2000 (The RIPA Policy);
  - monitoring and advising the Council on its "Whistleblowing" Policy;
  - determining appeals against public interest test decisions under the provisions of the Freedom of Information Act 2000;
  - granting exemptions to the restrictions attached to politically restricted posts; and
  - to be the Standards Committee for the Parish Councils in the district of South Staffordshire.
- 4.2.7 The Council has in place an Overview and Scrutiny process. Its remit includes the review of decisions and actions undertaken by the Council and scrutiny of all Key Decisions. Any matter arising from this process, in which fraud is suspected, can

*September, 2011*

be referred to South Staffordshire Internal Audit Section for independent investigation.

- 4.2.8 The Council's Audit Committee has included within its terms of reference a responsibility to review the effectiveness of internal audit including work in respect of fraud.
- 4.2.9 The Local Government Act 2000 as amended requires all members to give a written undertaking to comply with the Code of Conduct, if they are to remain on the Council.

#### 4.3 **Internal Control Systems**

- 4.3.1 The Council has a Scheme of Delegation, Procedure Rules, Financial Regulations, Accounting Procedures and various rules and codes of conduct in place. Staff are required to comply with this best practice when dealing with the Council's affairs.
- 4.3.2 The Director of Finance has a statutory responsibility under Section 151 of the Local Government Act 1972 as amended, to ensure proper arrangements are made for the Council's financial affairs. In addition, under the Accounts and Audit Regulations 2003 as amended by the Accounts and Audit Regulations (Amendment) 2006, the Council is required to maintain an adequate and effective internal audit of its financial records and systems of internal control.
- 4.3.3 The Council's aim is to have sound financial systems and procedures, which incorporate efficient and effective internal controls. The "separation of duties" is considered a fundamental control in such systems, especially when involving significant transactions. Directors are responsible for maintaining effective internal controls including the prevention and detection of fraud and other illegal acts. South Staffordshire Internal Audit Section will monitor and report upon these controls.
- 4.3.4 Internal Audit assesses regularly the level of risk within the Council with a view to preventing fraud and corruption. Departmental Risk Registers are also taken into account at this stage. Such assessments are discussed with Directors and, where appropriate, incorporated into work plans.
- 4.3.5 Significant emphasis has been placed on the thorough documentation of financial systems, and every effort is made to continually review and develop these systems in line with best practice to ensure efficient and effective internal controls and to include adequate separation of duties.
- 4.3.6 The adequacy and appropriateness of the Council's financial systems are independently monitored by both Internal and External Audit. Any weaknesses identified in internal control will be reported to management whose duty it will be to ensure that corrective action is taken. The Section 151 Officer can use his statutory power to enforce the required changes if necessary.
- 4.3.7 Directors will ensure that internal controls, including those in a computerised environment, are effectively maintained and documented and will investigate any potential weaknesses (e.g. in relation of the level of vacancies, sickness, absence and annual leave patterns).
- 4.3.8 It is evident across the country that an increasingly wide variety of frauds are being perpetrated. The larger frauds may involve the creation of multiple identities and false addresses, and involve different agencies.

*September, 2011*

4.3.9 Staff are therefore encouraged to liaise with those other agencies, exchanging information, where possible and appropriate to help prevent and detect such fraud. It is important that arrangements exist, and are developed, to encourage the exchange of information with other agencies including:

- Other Local and Statutory Authorities;
- Treasurers' Associations and Societies;
- Local, Regional and National Auditor Networks;
- Government Departments;
- Police Forces;
- The Audit Commission; and
- The National Anti-Fraud Network.

4.3.10 The Council has established formal procedures to respond to complaints received about any aspect of service delivery. Issues relating to fraud and corruption will be passed directly to the Internal Audit Manager.

4.3.11 The Council will involve the police to prosecute offenders where fraudulent or corrupt acts are discovered. This will be a matter for the S151 Officer and the Chief Executive to decide (NB Benefit Fraud will not normally involve the Police).

#### 4.4 **Working with Others**

4.4.1 There are a variety of arrangements in place, which facilitate the regular exchange of information between the Council and other local authorities and agencies, for the purpose of preventing and detecting fraud. These involve national, regional and local networks of investigators such as internal auditors, benefits investigators etc.

4.4.2 The Council is a member of the National Anti-Fraud Network (NAFN). NAFN provides access to information relating to fraud within the public sector. Fraud intelligence is collated and circulated to members, and information services to assist in the more effective investigation of fraud are available. We make use of these services.

4.4.3 As technologies develop, there is an ever increasing need to take advantage of the processing and analysis of data stored across the Council and beyond. This enables information and intelligence to be generated, which is a recognised means of preventing fraud and corruption.

4.4.4 The Audit Commission has drawn up a Code of Data Matching Practice for its National Fraud Initiative (NFI), which is recognised by the Information Commissioner as complying with Data Protection legislation.

4.4.5 The Council has 2 Fraud Hotlines (one for reporting fraud suspected within the Council – 01902 696252, and the other for reporting housing benefit fraud – 0500 658 008) to allow members of the public to report individuals who are suspected of committing fraud. There are a number of ways in which South Staffordshire Internal Audit can be contacted to report concerns of fraud and corruption, all of which are outlined in the Fraud and Corruption Response Procedure – see Appendix 1.

### 5. **Detection and Investigation**

*September, 2011*

- 5.1 It is the responsibility of the Strategic Management Team, Heads of Service and Service Managers to maintain good control systems and procedures, and to ensure that all staff comply with the instructions contained therein.
- 5.2 The Council's preventative systems, particularly internal control systems, provide indicators of fraudulent activity and are designed to deter any fraudulent activity.
- 5.3 It is often the alertness of Elected Members, Council Staff, and the general public to the possibility of fraud and corruption that enables detection to occur and appropriate action to take place.
- 5.4 Many frauds are discovered by chance, 'tip-off' or general audit work and arrangements are in place to enable such information to be properly dealt with, see Section 3.16.
- 5.5 Investigations are carried out in response to referrals of potential fraud. In addition proactive exercises target services areas identified as being at a high risk from fraud.
- 5.6 The Strategic Management Team, Heads of Service and Service Managers shall report to the Audit Manager all suspected irregularities, which could be instances of fraud. This is essential to our approach to fraud and corruption and ensures:
- consistent treatment of information regarding fraud and corruption
  - proper investigation by an independent and experienced audit team
  - the optimum protection of the Council's interests
- 5.7 When information relating to fraud or corruption is obtained it is reviewed and subject to a risk assessment. Some are followed up with a full investigation; others are better dealt with as management issues.
- 5.8 Depending on the nature and anticipated extent of the information obtained, South Staffordshire Internal Audit Services will normally work closely with:
- Strategic Management Team
  - Human Resources
  - Legal Services
  - Monitoring Officer
  - Other agencies, such as the Police and the Department for Work and Pensions
- This is to ensure that all allegations and evidence are properly investigated and reported upon, and that where appropriate, losses are recovered for the Council. Where appropriate this will include the use of Proceeds of Crime legislation.
- 5.9 Procedures for dealing with the investigation of fraud and corruption are included in the Fraud Manual of the Audit Section. Procedures and conduct for dealing with the investigation of benefit fraud are included in the Benefits Procedures Manuals.
- 5.10 The Council's Confidential Reporting (Whistle Blowing) Code provides a clear path for individuals to raise concerns of malpractice in any aspects of the Council's work, without the fear of recrimination or victimisation. The Council will take appropriate action to protect any individual who has raised a concern in good faith. The Code deals with the reporting of fraud or alleged fraud through formal channels, whether this is through Directorate management or Audit Manager.

*September, 2011*

- 5.11 Where fraud is found to have taken place with the involvement of a Council employee the Council's disciplinary procedure will be invoked.
- 5.12 Where financial impropriety is discovered relating to employees, members, or grant aided external organisations, the matter may be referred to the police in accordance with the Fraud Manual. Such decisions will be made by the Audit Manager in consultation with the Chief Executive and S151 Officer. Referral to the police will not necessarily prohibit action under the disciplinary procedure.
- 5.13 The Council's "Benefit Service Prosecution Policy" will be followed where the outcome of the investigation indicates benefit fraud. Where the Policy criteria is satisfied, offenders may be prosecuted or offered an alternative sanction in accordance with the Social Security Administration Act 1992, the Social Security Administration (Fraud) Act 1997 and 2001, the Fraud Act 2006 and the Welfare Reform Act 2007.
- 5.14 All investigations into suspected instances of fraud and corruption undertaken by the Council shall comply with the requirements of the Human Rights Act 1998, Regulation of Investigatory Powers Act 2000, Criminal Procedures and Investigation Act 1996 and have regard to the Police and Criminal Evidence Act 1984
- 5.15 The Council's External Auditor also has powers to independently investigate fraud and corruption.

## **6. Deterrence**

- 6.1 There are a number of ways in which we deter potential fraudsters from committing or attempting fraudulent or corrupt acts, whether they are inside or outside of the Council and these include :
- Publicising the fact the Council is firmly set against fraud and corruption and states this at every appropriate opportunity, e.g. statements in contracts, on claim forms, and in publicity literature.
  - Acting robustly and decisively when fraud and corruption is suspected and proven, e.g. the termination of contracts, the dismissal and/or prosecution of offenders.
  - Using all appropriate sanction action, including the Proceeds of Crime Act 2002.
  - Taking action to effect the maximum recoveries for the Council, e.g. through agreement, court action, penalties, insurance, superannuation etc. Where appropriate the Proceeds of Crime Act will be used to maximise the penalty suffered by the fraudster, and the level of recovery by the Council.
  - Having sound internal control systems, that still allow for innovation and calculated risk, but at the same time minimising the opportunity for fraud and corruption.
- 6.2 It is the responsibility of the Strategic Management Team and Heads of Service to communicate the Anti Fraud and Corruption Policy to their staff and to promote a greater awareness of fraud within their departments

## **7. Raising Fraud Awareness**

- 7.1 The Council recognises that the success and credibility of its Anti Fraud and Corruption Policy will depend largely on how effectively it is communicated throughout the organisation and beyond. Every opportunity will be taken to bring

*September, 2011*

it to the attention of staff, members and other stakeholders The Policy will also be shown on the Council's web page and be available on the Intranet.

- 7.2 Specifically, awareness is raised by a combination of face-to-face awareness sessions and publications about general and specific fraud issues.
- 7.3 The Council supports the concept of induction training, particularly for officers involved in internal control systems, to ensure that their responsibilities and duties in this respect are regularly highlighted and reinforced. The possibility of disciplinary action against officers who ignore such training and guidance is clear.
- 7.4 The officers involved in the review of internal control systems and investigative work will be properly and regularly trained. The training plans of South Staffordshire Internal Audit will reflect this requirement.
- 7.5 The officers involved in benefits investigative work will be properly and regularly trained. The training plans of the Benefit Fraud Team will reflect this requirement.
- 7.6 South Staffordshire Internal Audit Section offer programmes in Fraud Awareness, to promote the Anti Fraud and Corruption Policy and to give guidance on fraud prevention and detection.

## **8. Conclusions**

- 8.1 The Council has put into place a number of arrangements to protect itself from the risk of fraud. However in the current climate of change there are issues that will increase the risk of loss. Changes in structure, changes in systems and the de-layering of staff all contribute to our exposure to the risk of fraud. To mitigate against this risk the Council will regularly review arrangements
- 8.2 The Anti Fraud and Corruption Policy provides a framework for preventing and tackling fraudulent and corrupt acts against the Council. The approval of the Policy by the Audit Committee, on behalf of the Council, demonstrates the Council's commitment to protecting public funds and minimising losses to fraud and corruption. Having made this commitment, it is imperative that Directors put in place arrangements for disseminating the Policy and promoting fraud awareness, throughout their departments.

*September, 2011*

**SOUTH STAFFORDSHIRE COUNCIL**  
**MANAGING the RISK of FRAUD**  
**FRAUD and CORRUPTION RESPONSE PROCEDURE**

**The Practicalities - quick and easy reference**

1. Introduction and South Staffordshire Objective
2. The Council's Response
3. Reporting Suspicions
4. Roles and Responsibilities (who does what)

**Technical Detail**

5. Definition of Fraud and Corruption
6. The Investigation Process
7. Further Action

## The Practicalities

### 1. Introduction and Objective

- We are committed to protecting public funds. Minimising the losses to fraud and corruption is an essential part of ensuring that all of our resources are used for the purpose for which they are intended: the provision of high quality services to residents. We have a range of policies and procedures that facilitate this process. These include the: Anti Fraud and Corruption Policy, Prosecution and Sanction Policy; Whistle Blowing Policy; Surveillance Policy (RIPA) The Council's Constitution which form equally important parts of the Council's overall strategy.
- The public is entitled to expect the Council to conduct its affairs with integrity, accountability, honesty and openness, and demand the highest standards of conduct from those working for it and with it. Our overall objective is to identify and maintain good practices, address weaknesses in current processes and introduce improved systems for the management of those processes.
- Our Financial Regulations require that matters involving any suspected financial irregularities are referred to the Internal Audit Manager. The decision as to whether or not the irregularity should be investigated will be taken at his/her direction. All referrals are taken seriously and the action to be taken guided by an assessment of the risk. Where fraud is found appropriate disciplinary action and police involvement will be taken.
- This document is intended to provide direction and help to officers in dealing with suspected cases of theft, fraud and corruption. It also gives direction to others wanting to report matters of concern.

### 2. The Council's Response

- We have investigators based within South Staffordshire Internal Audit. They deal with internal fraud and corruption. Benefit Fraud is dealt with by the Benefit Investigation Team.
- The Council also provides a means of reporting concerns through its Whistle Blowing Policy
- Fraud and Corruption awareness is provided in various forms for all employees by the Internal Audit Section.

### 3. Reporting Suspicions

- If fraud or corruption is suspected, then employees are required to report this to the Internal Audit Manager. This should be the first action taken. They will then be provided with advice on how to proceed. Service Managers will be kept informed of issues arising, although this has to be sensitive to the involvement and potential conflict of interest of the individual manager.
- **Please be aware that any actions taken without prior consultation with Internal Audit could prejudice any subsequent investigation.**
- Contact can be made with the Internal Audit Section in a number of ways. These are:

For all general issues:

*September, 2011*

- Call Audit Manager on 01902 696611
- Email Audit via [J.Ordidge@sstaffs.gov.uk](mailto:J.Ordidge@sstaffs.gov.uk) or [internal.fraud@sstaffs.gov.uk](mailto:internal.fraud@sstaffs.gov.uk)
- phone the general fraud hotline on 01902 696252
- Write to South Staffordshire Internal Audit, South Staffordshire District Council Council Offices, Codsall, Wolverhampton, WV8 1PX

For benefit related issues:

- Call the Investigations Manager on 01902 696620
  - Email Benefit Fraud externally via [benefitsinvestigation@sstaffs.gov.uk](mailto:benefitsinvestigation@sstaffs.gov.uk)
  - Telephone the local benefit fraud hotline on 0500 658 008
  - Write to South Staffordshire Benefit Investigation Team, South Staffordshire District Council, Council Offices, Codsall, Wolverhampton, WV8 1PX.
  - Use the Council's Internet 'Report It' function.
- If in doubt, then Public Concern at Work will give free and totally independent advice on how to proceed. More information can be found in the Whistle Blowing Policy.

#### **4. Roles and Responsibilities (who does what)**

- S151 Officer (Director of Finance):

The Director of Finance has overall responsibility for the Council's response to fraud. It is his responsibility to oversee the action taken to investigate. In practice, much of this responsibility will normally be delegated to South Staffordshire Internal Audit Services.

- Strategic Management Team:

Each member of the Strategic Management Team has a responsibility for establishing and maintaining adequate system controls within their respective departments. This includes responsibility for the prevention and detection of fraud, including staff awareness of their responsibilities. They are responsible for implementing the requirements of the Council's overall strategy for combating fraud and corruption. In order to support this process they will disseminate the documents and policies that make up the strategy (referred to earlier)

- Heads of Service/Service Managers:

Heads of Service and Service Managers are in a position to take responsibility for the prevention and detection of fraud and corruption within their work area. They will encourage their staff to fulfil this objective. However, as soon as an officer suspects fraud or corruption they must report it as outlined in this document Reporting Suspicions

- Investigation Officers (Internal Audit Services/Benefit Fraud Team):

Allegations of potential fraud or corruption are risk assessed to form a view as to whether an investigation should be carried out. All investigations into fraud or corruption matters will be undertaken by Internal Audit or the Benefit Investigation Team for benefit fraud. Employees conducting investigations have powers which allow them access to various records and other information which may be deemed relevant.

*September, 2011*

- Employees:

All employees are required to act in accordance with the Staff Code of Conduct. Financial Regulations place responsibility for the prevention and detection of fraud with all employees. Any such concerns should be raised in accordance with Reporting Suspicions

- Members:

All Council Members are required to act in accordance with the Members Code of Conduct. Members also have a duty to report any issues of concern to the Director of Finance and the Monitoring Officer.

- Human Resources Staff:

Human Resources staff will provide advice to employees wishing to raise concerns. They will also provide advice to departmental officers in making decisions with regards to suspension and disciplinary proceedings. This includes matters covered in employment law and Council employment policies.

- Legal Officers:

Legal Services will be consulted, where appropriate, to advise on legal proceedings, including the recovery of assets.

- Communications Officers:

Corporate Communications will be informed of any high profile (or matters referred for prosecution by the Benefit Fraud Team) fraud cases so that they can manage or monitor the corporate media response.

## Technical Detail

### **5. Definition of Fraud and Corruption**

The Fraud Act of 2006 gives us a legislative definition of fraud as "the intention to make gain or cause loss by false representation, failing to disclose information or abuse of position".

***The Bribery Act 2010 defines bribery as "the giving or taking of a reward in return for acting dishonestly and/or in breach of the law. The reward could relate to money, payment in kind, goods or services".***

### **6. The Investigation Process**

- Where offences are suspected, investigations are carried out to establish the **facts** in an equitable and objective manner.
- The process will involve the use of authority or delegated powers to:
  - Screen allegations or information to gauge their credibility
  - Secure all evidence
  - Interview people suspected of being involved

September, 2011

- Interview witnesses
  - Take statements
  - Liaise with departments or other agencies (including the police)
- This work is conducted in accordance with legislation.

## **7. Further Action**

- Where evidence of offences or irregularities is found, the Council will consider taking further action.
- For Directorate issues:
  - Internal Audit will compile a report of its findings for submission to the department concerned, with a view to them deciding whether disciplinary action is appropriate.
  - Where appropriate, Internal Audit will liaise with the police in order for them to consider taking criminal action.
  - Internal Audit will advise departments on how to address procedural weaknesses identified during investigation.
- For benefit fraud issues:
  - Take action in accordance with the Benefit Fraud Prosecution and Sanction Policy.
  - Where an employee is involved in a benefit fraud consideration will be given to taking disciplinary action for breach of the staff Code of Conduct.
- For all types of fraud we will seek compensation for all losses incurred. This is done by:
  - Obtaining compensation orders or utilising the Proceeds of Crime Act in criminal cases.
  - Taking Civil proceedings in order to obtain a judgement.
  - Making deductions from superannuation contributions
  - Making deductions from benefit payments.
  - Making arrangements for voluntary payment.
  - Considering an insurance claim.
  - Considering any other means of recovery.

*September, 2011*

# **ANTI MONEY LAUNDERING POLICY**

**SOUTH STAFFORDSHIRE COUNCIL**  
**MANAGING the RISK of FRAUD**  
**ANTI-MONEY LAUNDERING POLICY**

**1.0 Foreword**

- 1.1 The public is entitled to expect the Council to conduct its affairs with integrity, honesty and openness and to demand the highest standards of conduct from those working for it. This Money Laundering Policy outlines the Council's commitment to creating an anti-fraud culture, and maintaining high ethical standards in its administration of public funds. It also recognises its responsibilities under the legislation including the Terrorism Act 2000, Proceeds of Crime Act 2002, Money Laundering Regulations 2007 and Fraud Act 2006 and subsequent regulations.

**2.0 Money Laundering**

- 2.1 Money laundering is a general term for any method of disguising the origin of "dirty" or criminal money. This money may be the proceeds of any criminal activity including terrorism, drugs trafficking, corruption, tax evasion and theft. The purpose of money laundering is to hide the origin of the dirty money so that it appears to have come from a legitimate source. Unfortunately no organisation is safe from the threat of money laundering, particularly where it is receiving funds from sources where the identity of the payer is unknown. It is, therefore, possible that South Staffordshire Council will be targeted by criminals wishing to launder the proceeds of crime.
- 2.2 In addition, it is possible that the proceeds of crime may be received from individuals or organisations that do not realise that they are committing an offence. It is no defence for the payer or the recipient to claim that they did not know that they were committing an offence if they should have been aware of the origin of the funds. All staff therefore dealing with the receipt of funds or having contact with third parties from whom funds may be received need to be aware of the possibility of money laundering taking place.
- 2.3 Under the legislation if staff assist an individual to launder funds from a criminal source they may be guilty of an offence and, if found guilty, could be subject to a fine or a prison sentence up to 14 years. It is important therefore that staff are aware of the rules and procedures that the Council has in place to ensure that they comply with the relevant legislation and approach taken by the Council as set out in this policy.
- 2.4 The Money Laundering Regulations require us to carry out 'Customer Due Diligence (CDD)'. Staff should therefore be alert to where the Council may be targeted by individuals trying to launder the proceeds of crime; avoid alerting anyone dealing with the Council that they have a suspicion that they may be attempting to launder, or have laundered, the proceeds of crime; and to report any suspicions of money laundering<sup>1</sup>.

*May, 2011*

- 2.5 Training will be provided to staff regarding Money Laundering to assist them in their awareness of how money laundering could take place and the appropriate method of dealing with this. In effect, any areas where money changes hands could therefore be at risk of money laundering attempts, i.e. application fees for taxi licences, planning applications, payment of council tax etc.
- 2.6 The Council already has procedures in place to limit the amount of cash that it receives, with other payment methods being made available. There are however instances where cash payments are continuing. To ensure however that the system is manageable, if a cash payment of less than £5,000 is received, then no identification checks will be needed.
- 2.7 Where the £5,000 limit is exceeded, officers dealing with the matter will need to establish the identity of the individual/company involved to seek to ensure that the risk of receiving the proceeds of crime can be minimised.
- 2.8 For individuals, their passport or photo driving licence should be provided, together with one of the following:
- Utility bills i.e. electricity, water etc. However mobile phone bills are not acceptable
  - Mortgage/building society/bank statements
  - Credit card statements
  - Pension or benefit books
- If passport or photo driving licence is not available, then two of the other items listed above will need to be produced.
- 2.9 For companies, a Companies House Search should be undertaken to confirm the existence of the company and identify who the directors are. Personal identification should then be obtained for the representatives of the company together with proof of their authority to act on behalf of the company. Care should be taken if it becomes clear that the individual has only recently become a director of the company or if there has been a recent change in the registered office.
- 2.10 For any other type of organisation, for example a sole trader or partnership, personal identification should be obtained for the individuals together with documents indicating their relationship to the organisation.
- 2.11 Copies of any evidence provided in support of the identification of an individual or organisation should be kept on a central file so that it can be referred to later if necessary. Records should be kept for 5 years after the end of the transaction.

### **Money Laundering Reporting Officer ("MLRO") and Money Laundering Compliance Officer ("MLCO")**

- 2.12 The Council's Money Laundering Reporting Officer ("MLRO") is the Director of Finance (Chief Financial Officer). The MLRO will be assisted by the Money Laundering Compliance Officer ("MLCO") who is the Accountancy and Financial Services Manager. The roles of both officers are set out in Appendix 1. Any suspicions that staff have must be reported to the MLCO.

## **Procedure for reporting suspicious transactions**

- 2.13 Any suspicious transactions which staff may become aware of in the course of their work must be reported to the Money Laundering Compliance Officer immediately using the Council's Internal Disclosure Form (see Appendix 2). Failure to make the appropriate report immediately will be regarded as gross misconduct and may result in dismissal without notice or pay in lieu of notice.
- 2.14 It is imperative that, if staff have a suspicion concerning an individual or organisation with which they are dealing that they do not alert them to that suspicion i.e. that no "tipping off" is done. Staff must, therefore, **not** make them aware that an internal disclosure report may be made. Once the report is made, the cash/cheques/other form of payment from this source should not be banked until clearance has been received from either the MLCO or MLRO. Such clearance may take up to seven days from the time when the initial report to the Money Laundering Compliance Officer is made.
- 2.15 If the funds are banked in this period without getting clearance from the MLCO or MLRO that staff member runs the risk of a fine and/or imprisonment for up to 14 years.

## **Additional guidance**

- 2.16 If you require any additional information or guidance in relation to the contents of this policy and your responsibilities please contact either the MLRO or MLCO. An Aide Memoir has been prepared – Appendix 3, which can be used as a brief reminder to staff of their responsibilities.

## **3.0 Conclusions**

- 3.1 The Council has put into place a number of arrangements to protect itself from the risk of money laundering. However in the current climate of change there are issues that will increase this risk. Changes in organisational structure, systems and staff all contribute to our exposure to the risk of money laundering. To mitigate against this risk the Council will regularly review arrangements
- 3.2 The Money Laundering Policy provides a framework for preventing and tackling money laundering acts against the Council. The approval of the policy by the Council demonstrates the Council's commitment to protecting public funds. Having made this commitment, it is imperative that the MLRO/MLCO put in place arrangements for disseminating the Policy and promoting money laundering awareness, throughout their departments.

### **Role of the Money Laundering Reporting Officer – “MLRO”**

The duties of the Money Laundering Reporting Officer are:

- To ensure that the Council complies with the requirements of the Money Laundering Regulations 2007 and the Proceeds of Crime Act 2002.
- To ensure that all relevant staff are aware of and comply with the Council's Money Laundering Policy.
- To ensure that the Council properly identifies all third parties dealing with the Council where there is a higher risk of the Council receiving the proceeds of crime and to ensure that copies of any documents taken as proof of evidence are kept on a central file by the Council.
- To ensure that all relevant staff receive training on how to identify, forestall and prevent money laundering.
- To ensure that all necessary disclosures to the Serious Organised Crime Agency (SOCA) are made and that they are made as soon as practically possible after the suspicion has been raised.
- To decide whether a suspicious transaction report requires a disclosure to be made to SOCA.
- To liaise with SOCA regarding the outcome of the disclosure and update staff accordingly.

### **Role of the Money Laundering Compliance Officer – “MLCO”**

The duties of the Money Laundering Compliance Officer are:

- To receive all suspicious transaction reports from employees of the Council.
- To assist the MLRO in preparing disclosure forms for forwarding to SOCA.
- To maintain a register of all disclosure made to SOCA showing the status of each disclosure.
- To maintain a file of all suspicious transaction reports received together with copies of the disclosure forms as appropriate.
- To notify the MLRO of any breaches of the Council's Money Laundering Policy, which come to his/her notice in the course of his/her work.

## APPENDIX 2

### **MONEY LAUNDERING – INTERNAL REPORTING FORM**

Money laundering legislation requires all individuals within the Council to report any knowledge or suspicions that they might have of money laundering (as defined in the Proceeds of Crime Act 2002) to the Council's Money Laundering Compliance Officer. To assist individuals the following pro forma has been developed. Particular circumstances may require different information to be disclosed and this should be fully explained, if applicable.

#### ***Instructions for completion***

*It is your legal duty and a requirement of your employment with South Staffordshire Council that you report any suspicion concerning proceeds of crime to:*

***Money Laundering Compliance Officer  
South Staffordshire Council  
Council Offices  
Wolverhampton Road  
Codsall  
Wv8 1PX***

***Tel: 01902 696607***

This should be marked **URGENT – PRIVATE AND CONFIDENTIAL TO THE ADDRESSEE ONLY.**

You are also reminded that **"Tipping-Off"** is a criminal offence. You should therefore avoid discussing the content of this report with anyone other than the Money Laundering Compliance Officer or Money Laundering Reporting Officer.

Date of Report:		Date suspicion first aroused:	
Prepared by: Name & Dept			
Disclosure Type:	(i.e. connections to crime/drugs/terrorism)		

**Main Subject (Person)**

Surname:		Forename(s):		Title:	
Date of Birth:		Gender:			
Occupation:		Employer:			
Address (in full)		Postcode	Home/Business/Registered	Current/Previous	

**Or**

**Main Subject (Company)**

Company Name:		Company No:		
Type of Business:		Vat No:		
Country of Reg:				
Address (in full)		Postcode	Home/Business/Registered	Current/Previous

**Bank Account Details**

Account Name:		Sort Code:	
Opened:		Account No:	
Closed:		Balance:	

**Other information**

Any knowledge/evidence held to confirm Identification and/or address, i.e. passport/driving licence etc:

**Connected Subject Person (if any)**

Surname:		Forename(s):		Title:	
Date of Birth:		Gender:			
Occupation:		Employer:			
Address (in full)		Postcode	Home/Business/Registered	Current/Previous	

**Or**

**Connected Subject Company (if any)**

Company Name:		Company No:			
Type of Business:		Vat No:			
Country of Reg:					
Address (in full)		Postcode	Home/Business/Registered	Current/Previous	

**Bank Account Details**

Account Name:		Sort Code:	
Opened:		Account No:	
Closed:		Balance:	

**Other information**

Any knowledge/evidence held to confirm Identification and/or address, i.e. passport/driving licence etc:

**Reason for the Suspicion**

**Please tick any or all of the following which might apply**

- |             |                          |                              |                          |           |                          |
|-------------|--------------------------|------------------------------|--------------------------|-----------|--------------------------|
| Drugs       | <input type="checkbox"/> | Personal tax fraud           | <input type="checkbox"/> | VAT fraud | <input type="checkbox"/> |
| Crime       | <input type="checkbox"/> | Company tax fraud            | <input type="checkbox"/> |           |                          |
| Immigration | <input type="checkbox"/> | Tobacco/Alcohol Excise fraud | <input type="checkbox"/> |           |                          |

**Following on from above, please set out the reason for the suspicion.**

Please continue on separate sheet if required

**Names of all other colleagues (principals & staff) who have been involved with the case**

**Declaration**

The above is an accurate account of the facts that are available to me at the time of making the report. If I become aware of additional information or changes to the information provided I will disclose these to the Money Laundering Compliance Officer in a timely manner. I am aware of the risks and penalties regarding "tipping-off" or frustrating in any way an investigation of the above or related matters by the authorities.

Signed:	_____	Date:	_____
Name in full:	_____	Position:	_____

## **APPENDIX 3**

### **MONEY LAUNDERING AVOIDANCE AIDE MEMOIR**

1. No member of staff must accept cash of more than £5,000 from any member of the public.
2. If you are offered cash of more than £5,000 you should advise the person offering it to you that it is not Council policy to accept large amounts of cash of more than £5,000 and that you need to obtain guidance from a senior member of staff. You should then contact the Money Laundering Compliance Officer/Money Laundering Reporting Officer to obtain authorisation to take the cash, if appropriate.
3. Any large cash sums should not be banked in the first instance. The Money Laundering Compliance Officer should be contacted to seek guidance as to how to deal with the funds. Forms to report the matter are included in the policy document at Appendix 2.
4. Whilst it is not acceptable to be suspicious of all cash based businesses, anyone whom you know to be associated with such a business should be dealt with using a higher degree of scepticism. If you have any reason to suspect the source of their funds then you should contact the Money Laundering Compliance Officer to discuss your concerns, even if the payment is not received in cash.
5. If you receive a complaint from a member of the public in relation to possible criminal activity being carried out by someone who may be a customer of the Council (i.e. a Council Tax or Business Rates payer, rent payer, licensee etc) you must pass this on to the Money Laundering Compliance Officer.



# **CONFIDENTIAL REPORTING ("WHISTLEBLOWING") POLICY**

# **CONFIDENTIAL REPORTING ("WHISTLEBLOWING") POLICY**

- 1.0 Introduction
- 2.0 What is "whistleblowing"
- 3.0 Aims and Scope of Policy
- 4.0 "Whistleblowing" Concerns as Distinct from "Grievances"
- 5.0 Safeguards
- 6.0 How to raise A Concern
- 7.0 How the Council will respond
- 8.0 How the matter can be taken further
- 9.0 The Responsible Officer
- 10.00 Other Relevant Policies

## **CONFIDENTIAL REPORTING ("WHISTLEBLOWING") POLICY**

### **1.0 INTRODUCTION**

- 1.1 Employees are often the first to realise that there may be something seriously wrong 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 malpractice.
- 1.2 The Council is committed to the highest possible standards of openness, probity and accountability. In line with that commitment we encourage employees and others with serious concerns about any aspect of the Council's work to come forward and voice those concerns. It is recognised that certain cases will have to proceed on a confidential basis. This policy document makes it clear that employees can do something without fear of reprisals. This Policy is intended to encourage and enable employees to raise serious concerns **within** the Council rather than overlooking a problem or "blowing the whistle" outside. It aims to provide employees with a safe alternative to silence.
- 1.3 The Standards Committee monitors and advises the Council on this Confidential Reporting Policy as part of the Council's commitment to ethical governance.

### **2.0 WHAT IS WHISTLEBLOWING?**

- 2.1 Whistleblowing is the popular term used when someone who works in or for an organisation (referred to in this document as an "employee") raises a concern about a possible fraud, crime, danger or other serious risk that could threaten customers, colleagues, the public or the organisation's own reputation.
- 2.2 As an early warning system, whistleblowing can help alert the Council to risks such as:-
  - a danger in the workplace;
  - fraud in, on or by the organisation;
  - mis-selling or price fixing;
  - offering, taking or soliciting bribes;
  - misreporting performance data;

### **3.0 AIMS AND SCOPE OF THIS POLICY**

- 3.1 This policy aims to:
  - provide avenues for employees to raise concerns and receive feedback on any action taken;
  - allow employees to take the matter further if they are dissatisfied with the Council's response;

- reassure employees that they will be protected from reprisals or victimisation for whistleblowing in good faith. Consideration will be given to redeployment if an employee requests it.

3.2 There are existing procedures in place to enable employees to lodge a grievance relating to their own employment. This policy is intended to cover concerns that fall outside the scope of other procedures.

That concern may be about something that:

- is unlawful; or
- is against the Council's Procedure Rules; or adopted policies or
- falls below established standards or practice; or
- amounts to improper conduct.

3.3 The Council is committed to the use of the whistleblowing policy to:

- deter wrongdoing;
- pick up potential problems early;
- enable critical information to get to the people who need to know and can address the issue;
- demonstrate to stakeholders, regulators and the court it is accountable and well managed;
- reduce the risk of anonymous and malicious leaks;
- minimise costs and compensation from accidents, investigations, litigation and regulatory inspections; and
- maintain and enhance its reputation.

#### **4.0 "WHISTLEBLOWING" CONCERNS AS DISTINCT FROM "GRIEVANCES"**

4.1 Whistleblowing is where an employee has a concern about danger or illegality that has a public interest aspect to it: usually because it threatens others (e.g. customers, or the public). A grievance or private complaint is, by contrast, a dispute about the employee's own employment position and has no additional public interest dimension.

4.2 The Council recognises that there may be occasions where a whistleblowing issue may be entangled with a grievance. Further advice on this can be obtained in confidence from the Human Resources Manager (01902 696103) or the Internal Audit Manager (01902 696611).

#### **5.0 SAFEGUARDS**

##### ***5.1 Harassment or Victimisation***

The Public Interest Disclosure Act, (PIDA) is often referred to in the UK as the "whistleblowing law". The Act provides that employers should not victimise any worker who reports a matter in one of the ways set out in the legislation. The Council recognises that the decision to report a concern can be a difficult one to

*May, 2011*

make, not least because of the fear of reprisal from those responsible for the malpractice. The Council will not tolerate harassment or victimisation and will take action to protect an employee who raises a concern in good faith. The Council will not tolerate any reprisal against an employee who has raised a concern under the Whistleblowing Policy and will treat any such reprisal as a disciplinary matter which may lead to dismissal. These assurances are not extended to employees who maliciously raise a concern he or she knows to be false.

5.2 This does not mean that if an employee is already the subject of disciplinary or redundancy procedures, that those procedures will be halted as a result of their whistleblowing.

### 5.3 ***Confidentiality***

The Council will do its best to protect an employee's identity when he/she raises a concern and do not want his/her name to be disclosed. It must be appreciated that the investigation process may reveal the source of the information and a statement by the employee may be required as part of the evidence.

### 5.4 ***Anonymous Allegations***

This policy encourages employees to put their name to your allegation. Concerns expressed anonymously are much less powerful, but they will be considered at the discretion of the Council.

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

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

### 5.6 ***Untrue Allegations***

If an employee make an allegation in good faith, but it is not confirmed by the investigation, no action will be taken against him/her. If, however, an employee make allegations that are malicious or simply to cause anger, irritation or distress, disciplinary action may be taken against the employee making the allegations.

5.7 While openness is the ideal, the Council recognises that in practice some employees will have good reason to feel anxious about identifying themselves at the outset. Therefore the Council undertakes to ensure their name will not be revealed without their consent, unless required by law. The Council cannot however guarantee even though an employee's name will not be mentioned, that others will not try to deduce (correctly or otherwise) their identity.

## **6.0 HOW TO RAISE A CONCERN**

6.1 You should raise your concern with the Internal Audit Manager, or in his/her absence, a member of the Internal Audit Team. Where an employee feels unable to raise concerns with the Internal Audit Manager, they can raise their concern with their line manager, who must immediately inform the Internal Audit Manager. Under no circumstances should any investigation be undertaken by the Manager.

- 6.2 If the concern raised relates to fraud or corruption, then the matter will be reviewed and investigated by Internal Audit. If however, the concern relates to a management issue, then the matter will be recorded and forwarded onto the appropriate officer to deal with it. If the issue involves a member of the Council, the matter will also be forwarded to the Monitoring Officer (Head of Governance and Scrutiny Services).
- 6.3 Concerns are best raised in writing. Setting out the background and history of the concern, giving names, dates and places where possible, and the reason why you are particularly concerned about the situation. If an employee does not feel able to put your particular concern in writing, they can telephone or meet the appropriate officer. The officer notified of an individuals concern must record those concerns taking a statement where they feel it appropriate.
- 6.4 In addition, **a confidential reporting hotline (01902 – 696252)** and **e.mail address (internal.fraud@sstaffs.gov.uk)** have been set up to facilitate the reporting of any concerns. Employees using either facility should provide as much information as possible to ensure the concern can be properly investigated, including leaving their name and contact number, if possible.
- 6.5 The earlier concerns are raised, the easier it is to take action, and although the complainant will not be expected to prove the truth of the allegation, he/she need to be able to demonstrate to the person contacted that there are sufficient grounds for concern.
- 6.6 Advice and guidance on how matters of concern may be pursued can be obtained from the **Internal Audit Manager (01902 – 696611)** (alternatively, for employment related matters from the Human Resources Manager (01902 – 696103) or in cases involving Councillors from the Monitoring Officer (01902 – 696108)).
- 6.7 An employee may invite his/her trade union or professional association to raise a matter on his/her behalf.

## **7.0 HOW THE COUNCIL WILL RESPOND**

- 7.1 The action taken by the Council will depend on the nature of the concern. The matters raised may:
- be investigated internally
  - be referred to the Police
  - be referred to the external Auditor
  - form the subject of an independent inquiry
- 7.2 In order to protect individuals and the Council, initial enquires will be made to decide whether an investigation is appropriate and, if so, what form it should take. Concerns or allegations which fall within the scope of specific procedures will normally be referred for consideration under those procedures.
- 7.3 Some concerns may be resolved by agreed action without the need for investigation.
- 7.4 Within ten working days of a concern being received, the Council will write to you:
- acknowledging that the concern has been received;
  - indicating how it proposes to deal with the matter;
  - giving an estimate of how long it will take to provide a final response;

- advising you whether any initial enquiries have been made; and
- advising you whether further investigations will take place, and if not, why not.

7.5 The amount of contact between the officers considering the issues and the employee raising the concern, will depend on the nature of the matters raised the potential difficulties involved and the clarity of the information provided. If necessary, further information will be sought from the employee making the allegation.

7.6 When any meeting is arranged, an employee has the right, if he/she so wishes, to be accompanied by a Trade Union or professional association representative or a friend who is not involved in the area of work to which the concern relates.

7.7 The Council will take steps to minimise any difficulties which an employee may experience as a result of raising a concern. For instance, if an employee is required to give evidence in criminal or disciplinary proceedings, the Council will advise him/her about the procedure.

7.8 The Council accepts that employees need to be assured that the matter has been properly addressed. Thus, subject to legal constraints, the employee raising the concern will receive information about the outcomes of any investigations.

## **8.0 HOW THE MATTER CAN BE TAKEN FURTHER**

8.1 This policy is intended to provide employees with an avenue to raise concerns. The Council hopes employees will be satisfied with it. If they are not, they are always entitled to take the matter up outside the Council; the following are possible contact points:

- your local Councillor (if you live within South Staffordshire)
- the external Auditor (see para. 4.5)
- the Council's formal complaints procedure
- relevant professional bodies or regulatory organisations
- your solicitor
- the Police

8.2 If employees do take the matter outside the Council, they will need to ensure that they do not disclose confidential information or that disclosure would be privileged.

## **9.0 THE RESPONSIBLE OFFICER**

9.1 The Monitoring Officer has overall responsibility for the maintenance and operation of this policy. Internal Audit maintain a record of concerns raised and the outcomes (but in a form which does not endanger your confidentiality) and will report as necessary to the Monitoring Officer and/or the Standards Committee.

## **10.0 OTHER RELEVANT POLICIES**

10.1 There are other policies and procedures, which may be used to support this policy, and these are listed below. These policies are available on the Intranet or from Human Resources.

- Financial Regulations and Procedure Rules
- Anti Fraud and Corruption Policy and Guidelines
- Harassment Policy

- Benefits Services Prosecution Policy
- Equal Opportunities Policy
- Disciplinary and Grievances Procedures
- Code of Conduct for Officers
- Code of Conduct for Councillors



# **INTERNET ACCEPTANCE USAGE POLICY**

## **1. POLICY STATEMENT**

South Staffordshire Council will ensure all users of Council provided internet facilities are aware of the acceptable use of such facilities.

Each user on being given Internet usage is required to sign a "user agreement" form indicating that they have read and understood this policy.

## **2. PURPOSE**

This policy document tells you how you should use your Council Internet facility. It outlines your personal responsibilities and informs what you must and must not do.

The Internet facility is made available for the business purposes of the Council. A certain amount of personal use is permitted in accordance with the statements contained within this Policy.

It is recognised that it is impossible to define precise rules covering all Internet activities available and adherence should be undertaken within the spirit of the policy to ensure productive use of the facility is made.

## **3. SCOPE**

This policy applies to all users of South Staffordshire Council's owned and operated computer systems and networks located in Council premises.

Users covered by this document are employees, elected members and any third parties granted access to the Council's Internet facilities including, contractors, sub-contractors, agents, temporary or casual workers, work experience placements and those from voluntary organisations.

## **4. DEFINITION AND DISTRIBUTION**

A copy of the policy will be provided to new starters via induction when they are given access to the Internet. Existing users will be issued with a copy and all employees will be notified of any changes to the policy by an e-mail that directs them to the latest version on the Intranet.

It is the users responsibility to ensure that they are fully conversant with, and comply with, such amendments on notification of any change.

## **5. RISKS**

South Staffordshire Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- The non-reporting of information security incidents,
- Inadequate destruction of data
- The loss of direct control of user access to information systems and facilities etc.

*May, 2011*

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

## **6. APPLYING THE POLICY**

Internet skills are recognised by the Council as a core competency. Any new employee must attend an I.T. induction course. The Training Officer will arrange a date for the course.

The use of South Staffordshire Council's Internet systems is intended for South Staffordshire Council business within the broad objectives of the Council.

### **6.1 Personal Use**

Reasonable personal use of the Internet is allowed during non-working hours. Personal usage does not include use for private business purposes as this is prohibited at all times for employees and third parties.

Elected members may use the Internet for private business purposes for reasonable periods.

Personal use, for instance booking reservations or tickets or purchase of any goods or services will be limited to non-working hours in other words "off the clock". The Council's Internet facility should not be used for personal downloading purposes.

### **6.2 Inappropriate Use**

Viewing, archiving, storage, distribution, editing or recording of websites that contain inappropriate material is strictly forbidden, this includes pornography, instructions on criminal or terrorist skills, promotion of cults, gambling, or any other material or statements which are likely to cause offence to others or to bring the Council into disrepute. Any form of inappropriate use is forbidden at all times on the Council's computer systems and networks.

Employees or elected members who accidentally access such material should immediately close down their browser and report the incident, for their own protection, to the Help Desk.

Any employee who discovers or observes a violation of this policy should notify their Line Manager, Head of Service, Service Manager or Director immediately. Any elected member who discovers or observes a violation of this policy should notify the I.C.T. Services Manager or Network Manager immediately.

The Council acknowledges that access to sites of a potentially contentious nature may be appropriate in some areas. The Council however places a special responsibility of care on elected members, managers and employees operating in such areas to ensure that such access is necessary and that employees, elected members and members of the community are not exposed to such material.

Employees or elected members should not use the Internet to conduct transactions in pursuit of their own commercial or business interests nor in such a way that the Council could be implicated in such transactions.

*May, 2011*

Employees or elected members should not use the Council's Internet facility to gain access to remote sites or equipment either owned by them or in pursuit of their own commercial or business interests under any circumstances.

Employees or elected members are not allowed to access chat lines or social networks such as Facebook or newsgroups and no attempts should be made to access such web sites at any time in compliance with the Council's Social Media Policy.

Any information stored by an employee on Council equipment may be subject to disclosure in the event of a request under the Freedom of information Act and must comply with the Data Protection Act.

### **6.3 Downloading**

Employees or elected members must not transmit copyright software or files from their computer via the Internet.

Employees or elected members must not knowingly use the Internet to download pirated software or data. The use of file sharing or peer to peer software is strictly prohibited. Peer to peer allows Internet users to transfer files directly, rather than through the use of a website or directory.

The downloading of software programs, music, videos, screen savers, utilities or software extensions is strictly prohibited. Files should only be downloaded when required for the performance of work. The employee should contact I.C.T. Services who will make the necessary arrangements.

### **6.4 Viruses**

Viruses damage computer systems, destroy data, cause disruption and incur considerable expense for the Council. The Council ensures that each computer has an appropriate virus scanner and that this is regularly updated. All software and files downloaded from the Internet will be virus checked.

Employees or elected members are expected to take all reasonable precautions to ensure that all software and files placed on media brought into the Council, either through downloading on site or at home, is virus free.

Employees or elected members must not use the Council's Internet facility to deliberately propagate any virus worm, Trojan horse, spyware, malware or back door program code.

No employee or elected member may use the Council's Internet facilities knowingly to disable or overload any computer system or our network.

### **6.5 Internet Access Control**

The Council has no control over the content of external sites. However to protect its employees and elected members from being subject to inappropriate or offensive materials web filtering software is used.

This software is used to record all Internet usage. We want you to be aware that our security systems constantly record (for each and every user) each Internet site visit or attempted visit and each file transfer into and out of our internal networks, and we

*May, 2011*

reserve the right to do so at any time. No employee or elected member should have any expectation of privacy as to his or her Internet usage.

Managers may review Internet activity reports and analyse usage patterns, and they may choose to publicise this data to assure that Council's Internet resources are devoted to maintaining the highest levels of productivity.

## **6.6 Internet Account Management, Security and Monitoring**

The Council will provide a secure logon-id and password facility for your Internet account. The Council's ICT Service Unit is responsible for the technical management of this account.

You are responsible for the security provided by your Internet account logon-id and password. Only you should know your log-on id and password and you should be the only person who uses your Internet account.

The provision of Internet access is owned by the Council and all access is recorded, logged and interrogated for the purposes of:

- Monitoring total usage to ensure business use is not impacted by lack of capacity.
- The filtering system monitors and records all access for reports that are produced for line managers and auditors.

## **6.7 Acceptable Usage Policy**

Each user must read, understand and sign to verify they have read and accepted this policy.

I understand and agree to comply with the Internet Acceptable Usage Policy of my organisation.

## **7. POLICY COMPLIANCE**

Compliance with this policy and guidelines will be monitored. Any breach of this policy may result in disciplinary action being taken. Access may be withdrawn at any time as a result of, or pending the outcome of, investigations into suspected misuse.

Any misuse that is found to be illegal will be reported to the appropriate authorities and may result in civil or criminal action.

If you do not understand the implications of this policy or how it may apply to you, seek advice from ICT Services.

## **8. POLICY GOVERNANCE**

The following table identifies who within South Staffordshire Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

*May, 2011*

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

<b>Responsible</b>	ICT Services Manager
<b>Accountable</b>	Section 151 Officer
<b>Consulted</b>	HR Manager, Data Protection Officer, Director of Legal and Public Health Protection Services, Network Manager, Monitoring Officer
<b>Informed</b>	Senior Management Team, Service Managers

## 9. REVIEW AND REVISION

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the ICT Services Manager.

## 10. REFERENCES

The following South Staffordshire Council policy documents are directly relevant to this policy, and are referenced within this document:

- Computer Misuse Act 1990
- Data Protection Act 1998
- Part 3 of the Data Protection Code on Employment Practices - "Monitoring at Work"
- Human Rights Act
- Freedom of Information Act
- Regulation of Investigatory Powers Act 2000
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Employees Handbook
- Security Policy
- Email Policy

## 11. KEY MESSAGES

- Users must familiarise themselves with the detail, essence and spirit of this policy before using the Internet facility provided.
- At the discretion of your Service Manager and provided it does not interfere with your work, the Council permits personal use of the Internet in your own time (for

*May, 2011*

example during your lunch-break). **Employees must be clocked out for personal use and need to be aware that failure to do so will be interpreted as that they are undertaking personal use during the paid time and service of the Council.**

- Users are responsible for ensuring the security of their Internet account logon-id and password. Individual user log-on id and passwords should only be used by that individual user, and they should be the only person who accesses their Internet account.
- Users **must not** create, download, upload, display or access knowingly, sites that contain pornography or other “unsuitable” material that might be deemed illegal, obscene or offensive.
- Users must assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.

*May, 2011*



# **EMAIL USAGE POLICY**

## **1. POLICY STATEMENT**

The Council recognises email as one of the major means of communication. It actively promotes its use as a trusted, efficient and environmentally friendly form of communication.

## **2. PURPOSE**

Any unauthorised access to email or false, defamatory, discriminatory or offensive comments distributed through the Council's email system may result in litigation by individuals or organisations. The policy is therefore designed to protect both the Council and its employees from legal and human resource management issues while using the Council's email system.

The objective of this Policy is to direct all users of Council email facilities by:

- Providing guidance on expected working practice.
- Highlighting issues affecting the use of email.
- Informing users about the acceptable use of ICT facilities in relation to emails.
- Describing the standards that users must maintain.
- Stating the actions that may be taken to monitor the effectiveness of this policy.
- Warning users about the consequences of inappropriate use of the email service.

The Policy establishes a framework within which users of Council email facilities can apply self-regulation to their use of email as a communication and recording tool.

## **3. SCOPE**

This policy applies to all users of South Staffordshire Council owned and operated computer systems and networks irrespective of the location it is used from.

Users covered by this document are employees, elected members and any third parties granted access to the Council's email facilities including, contractors, sub-contractors, agents, temporary, agency and casual workers, work experience placements and those from voluntary organisations.

## **4. DEFINITION**

All email prepared and sent from South Staffordshire Council email addresses or mailboxes, and any non-work email sent using South Staffordshire Council ICT facilities is subject to this policy.

## **5. DISTRIBUTION**

A copy of the policy will be provided to new starters via induction when they are given access to the Council's email system. Existing users will be notified of any changes to the policy by an email that directs them to the latest version on the Intranet. It is the users responsibility to ensure that they are fully conversant with, and comply with, such amendments on notification of any change.

## **6. RISKS**

South Staffordshire Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- The non-reporting of information security incidents.
- Inadequate destruction of data.
- The loss of direct control of user access to information systems and facilities.
- The loss of or inappropriate dissemination of data.
- Litigation by individuals or organisations due to unauthorised access to email or false, defamatory, discriminatory or offensive comments distributed through the Council's email system.
- Misuse of the Council's facilities.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

## **7. APPLYING THE POLICY**

### **7.1 Acceptable Purpose**

Email skills are recognised by the Council as a core competency. Any new employee must attend an I.T. induction course. The Training Officer will arrange a date for the course. The use of South Staffordshire Council's email systems is intended for South Staffordshire Council business within the broad objectives of the Council.

Personal usage should be limited to non-working hours (eg lunch etc). Reasonable personal use of email services is allowed but as a privilege and not a right. Personal usage does not include use for private business purposes as this is prohibited at all times.

Email services shall not be used for intentionally viewing, archiving, storage, distribution, editing or recording of threatening, obscene, harassing or derogatory material; or transmittal of material that is confidential to the Council (e.g. membership lists, accounting records, business plans, etc) or the distribution of spam/junk mail.

Use of the email systems to receive (download) software programs, utilities or software extensions is prohibited without prior authorisation from South Staffordshire Council's Network Manager or I.C.T. Service Manager. This includes (but is not limited to) screen savers, games, and utility programs. It does not include files such as Word documents, Excel documents, Adobe Portable Document Format (PDF) files.

### **7.2 Monitoring of email**

The Council may monitor any email messages sent or received and Outlook Calendars. This includes personal emails sent via the Council's facilities, which will be subject to the same level of monitoring as Council related email and Private Outlook appointments.

The content of all incoming and outgoing emails will be scanned for potential viruses.

An activity log of all outgoing and incoming emails will be maintained primarily for email server management, statistical and reporting purposes. This log will include the email subject line, sender and destination addresses, date and time stamp information.

If misuse of the email system is suspected then activity logs may, in accordance with this policy, be viewed by the individual's line manager and /or Internal Audit and Human Resources. This may be extended to the selective examination of individual email messages if there are reasonable grounds for suspecting that it will reveal evidence that the employee has violated this policy. This includes reading personal emails sent or received using the Council's facilities.

Under the Data Protection Act 1998 all users are allowed access to any logged personal data. Requests for copies of this data must be made, via email, to the I.C.T. Service Manager who will respond within 10 working days of the request.

Emails remain on security copies available for inspection for a minimum of 60 days.

Any employee who discovers a violation of this policy should notify their Line Manager, Head of Service, Service Manager or Director immediately, if necessary the Whistleblowing Policy.

### **7.3 Email as Records**

All emails that are used to conduct or support official South Staffordshire Council business must be sent using a "@sstaffs.gov.uk" address. All emails sent via the Government Connect Secure Extranet (GCSx) must be of the format "@sstaffs.gcsx.gov.uk".

Non-work email accounts **must not** be used to conduct or support official South Staffordshire Council business. Councillors and users must ensure that any emails containing sensitive information must be sent from an official council email. Any emails containing PROTECT or RESTRICTED information must be sent from a GCSx email. All emails that represent aspects of Council business or Council administrative arrangements are the property of the Council and not of any individual employee.

Emails held on Council equipment are considered to be part of the corporate record and email also provides a record of staff activities.

### **7.4 Email as a Form of Communication**

Email is designed to be an open and transparent method of communicating. However, it cannot be guaranteed that the message will be received or read, nor that the content will be understood in the way that the sender of the email intended. It is therefore the responsibility of the person sending an email to decide whether email is the most appropriate method for conveying time critical or PROTECT or RESTRICTED information or of communicating in the particular circumstances.

Users must ensure that any emails containing sensitive information must be sent from an official council email. Any emails containing PROTECT or RESTRICTED information must be sent from a GCSx email.

Email must not be considered to be any less formal than memo's or letters that are sent out from a particular service or the authority. When sending external email, care should be taken not to contain any material which would reflect poorly on the Council's reputation or its relationship with customers, clients or business partners.

Under no circumstances should users communicate material (either internally or externally), which is, for example, defamatory, obscene, or does not comply with the Council's Equal Opportunities Policy or which could reasonably be anticipated to be considered inappropriate. Any user who is unclear about the appropriateness of any material, should consult the Communications Officer prior to commencing any associated activity or process.

IT facilities provided by the Council for email should not be used:

- For the transmission of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations.
- For the unauthorised transmission to a third party of PROTECT or RESTRICTED material concerning the activities of the Council.
- For the transmission of material such that this infringes the copyright of another person, including intellectual property rights.
- For activities that unreasonably waste staff effort or use networked resources, or activities that unreasonably serve to deny the service to other users.
- For activities that corrupt or destroy other users' data.
- For activities that disrupt the work of other users.
- For the creation or transmission of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material.
- For the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
- For the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others.
- For the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- For the creation or transmission of defamatory material.
- For the creation or transmission of material that includes false claims of a deceptive nature.
- For so-called 'flaming' - i.e. the use of impolite terms or language, including offensive or condescending terms.
- For activities that violate the privacy of other users.
- For unfairly criticising individuals, including copy distribution to other individuals.
- For publishing to others the text of messages written on a one-to-one basis, without the prior express consent of the author.
- For the creation or transmission of anonymous messages - i.e. without clear identification of the sender.
- For the creation or transmission of material which brings the Council into disrepute.

## **7.5 Junk Mail**

There may be instances where a user will receive unsolicited mass junk email or spam. It is advised that users delete such messages without reading them. Do not reply to the email. Even to attempt to remove the email address from the distribution list can confirm the existence of an address following a speculative email.

Before giving your email address to a third party, for instance a website, consider carefully the possible consequences of that address being passed (possibly sold on) to an unknown third party, and whether the benefits outweigh the potential problems.

Chain letter emails (those that request you forward the message to one or more additional recipients who are unknown to the original sender) **must not** be forwarded using South Staffordshire Council systems or facilities.

## **7.6 Mail Box Size**

In order to ensure that the systems enabling email are available and perform to their optimum, users should endeavour to avoid sending unnecessary messages. In particular, the use of the "global list" of email addressees is discouraged.

Users are provided with a limited mail box size of 35Mb to reduce problems associated with server capacity. Email users should manage their email accounts to remain within the limit, ensuring that items are filed or deleted as appropriate to avoid any deterioration in systems.

Email messages can be used to carry other files or messages either embedded in the message or attached to the message. If it is necessary to provide a file to another person, then a reference to where the file exists should be sent rather than a copy of the file. This is to avoid excessive use of the system and avoids filling to capacity another person's mailbox. If a copy of a file must be sent then it should not exceed 9Mb in size.

## **7.7 Categorisation of Messages**

When creating an email, the information contained within it must be assessed and classified by the owner according to the content, when appropriate. It is advisable that all emails are protectively marked in accordance with the HMG Security Policy Framework (SPF). The marking classification will determine how the email, and the information contained within it, should be protected and who should be allowed access to it.

The SPF requires information to be protectively marked into one of 6 classifications. The way the document is handled, published, moved and stored will be dependant on this scheme.

The classifications are:

- Unclassified.
- PROTECT.
- RESTRICTED.
- CONFIDENTIAL.
- SECRET.
- TOP SECRET.

Information up to RESTRICTED sent via GCSx must be marked appropriately using the SPF guidance.

## **7.8 Security**

Users are responsible for ensuring that their email remains secure and all email sent is the responsibility of the sender. Therefore users are responsible for the security of their password(s) and must lock their PC when leaving their desk for a prolonged period.

Users must not use someone else's unattended PC to send email, or find any other method to send mail that is not clearly identified as from them. Certain users may be granted

permission to access other email accounts and send messages on behalf of those users, but such mail must be clearly identified as from the third party.

Although anti-virus software is installed to minimise the risk of users receiving email infected with a virus, it is still the user's responsibility to contact I.C.T. Services before attempting to open an email attachment that looks suspicious or if there is any question about the content or sender.

NEVER OPEN AN EMAIL IF YOU ARE IN DOUBT. CONTACT I.C.T. SERVICES IMMEDIATELY.

### **Signatures**

All outgoing emails being sent from the Council's email system will have a signature that contains the following:

Name  
Job Title  
Service Unit  
Work telephone number  
Fax number  
Email address

### **Disclaimers**

All outgoing emails being sent from the Council's email system will have the following legal disclaimer added to it automatically at the end:

This transmission is confidential and may be privileged.

This transmission is intended for the named addressee(s) only and may contain sensitive or protectively marked material up to RESTRICTED and should be handled accordingly. Unless you are the named addressee (or authorised to receive it for the addressee) you may not copy or use it, or disclose it to anyone else. If you have received this transmission in error please contact the sender at:

All GCSX traffic may be subject to recording and/or monitoring in accordance with relevant legislation.

This message is confidential and may be privileged. It is intended for the addressee(s) only. If you are not a named addressee, you may not use or copy it or disclose it to any other person. If you receive this message in error, please contact the sender at:

### **When sending a personal email, the following statement should be added:**

This email is personal. It is not sent on behalf of South Staffordshire Council.

Emails sent between sstaffs.gov.uk address are held with the same network and are deemed to be secure. However, emails that are sent outside this closed network travel over the public communications network and are liable to interception or loss. There is a risk that copies of the email are left within the public communications system. Therefore, PROTECT and RESTRICTED material must not be sent via email outside a closed network, unless via the GCSx email.

Where GCSx email is available to connect the sender and receiver of the email message, this **must be used** for all external email use and must be used for communicating PROTECT and RESTRICTED material.

**All Council employees that require access to GCSx email must read, understand and sign the GCSx Acceptable Usage Procedure and Personal Commitment Statement.**

## **7.9 Confidentiality**

Staff must make every effort to ensure that the confidentiality of email is appropriately maintained. Staff should be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies. Moreover, confidentiality cannot be assured when messages are sent over outside networks, such as the Internet, because of the insecure nature of most such networks and the number of people to whom the messages can be freely circulated without the knowledge of South Staffordshire Council.

Care should be taken when addressing all emails, but particularly where they include PROTECT or RESTRICTED information, to prevent accidental transmission to unintended recipients. Particular care should be taken if the email client software auto-completes an email address as the user begins typing a name.

Automatic forwarding of email (for example when the intended recipient is on leave) must be considered carefully to prevent PROTECT or RESTRICTED material being forwarded inappropriately. Rules can be implemented to include or exclude certain mail based on the sender or subject. If you require assistance with this, please contact the ICT Services Manager in the first instance.

The automatic forwarding of a GCSx email to a lower classification email address (i.e. a standard .gov.uk email) contradicts national guidelines and is therefore not acceptable.

## **Data Protection**

The inclusion in an email of personal data, such as name, phone number, email address, is deemed to be "processing" personal data by the Data Protection Act 1998. Users should be conversant with the Act where appropriate (The Council's Data Protection Officer can be contacted for further information on Ext 6114).

## **Freedom Of Information Act**

Any information stored by an employee on Council equipment may be subject to disclosure in the event of a request under the Freedom of information Act.

## **7.10 Negligent Virus Transmission**

Computer viruses are easily transmitted via email and internet downloads. Full use must therefore be made of South Staffordshire Council's anti-virus software. If any user has concerns about possible virus transmission, they must report the concern to the Network Manager.

In particular, users:

- Must not transmit by email any file attachments which they know to be infected with a virus.
- Must not download data or programs of any nature from unknown sources.
- Must ensure that an effective anti-virus system is operating on any computer which they use to access Council facilities.
- Must not forward virus warnings other than to ICT Services.
- Must report any suspected files to the ICT helpdesk.

In addition, the Council will ensure that email is virus checked at the network boundary and at the host, and where appropriate will use two functionally independent virus checkers.

If a computer virus is transmitted to another organisation, the Council could be held liable if there has been negligence in allowing the virus to be transmitted. Users must therefore comply with the Software Policy.

## 8. POLICY COMPLIANCE

Compliance with this policy and guidelines will be monitored by I.C.T. Services. Any breach of this policy may result in disciplinary action being taken. Unacceptable levels of personal use of the Council's email system may also be regarded as misuse and be treated as a disciplinary matter. Access may be withdrawn at any time as a result of, or pending the outcome of, investigations into suspected misuse.

Any misuse, which is found to be illegal, will be reported to the appropriate authorities and may result in civil or criminal action.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the ICT Services Manager.

## 9. POLICY GOVERNANCE

The following table identifies who within South Staffordshire Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

<b>Responsible</b>	ICT Services Manager
<b>Accountable</b>	Section 151 Officer
<b>Consulted</b>	HR Manager, Data Protection Officer, Director of Legal and Public Health Protection Services, Network Manager, Monitoring Officer
<b>Informed</b>	Senior Management Team, Service Managers

## 10. REVIEW AND REVISION

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the ICT Services Manager.

## 11. REFERENCES

The following documents are directly relevant to this policy, and are referenced within this document:

Computer Misuse Act 1990

Data Protection Act 1998

Part 3 of the Data Protection Code on Employment Practices - "Monitoring at Work"

Human Rights Act

GCSx Acceptable Use Procedures

Freedom Of Information Act

Regulation of Investigatory Powers Act(RIPA) 2000

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Employees Handbook

Security Policy

Internet Policy

## 12. KEY MESSAGES

- All emails that are used to conduct or support official South Staffordshire Council business must be sent using a "@sstaffs.gov.uk" address.
- All emails sent via the Government Connect Secure Extranet (GCSx) must be of the format "@sstaffs.gcsx.gov.uk".
- Non-work email accounts must not be used to conduct or support official South Staffordshire Council business.
- Users must ensure that any emails containing sensitive information must be sent from an official council email.
- All official external email must carry the official Council disclaimer.
- Under no circumstances should users communicate material (either internally or externally), which is defamatory, obscene, or does not comply with the Council's Equal Opportunities policy.
- **When sending private emails employees must be clocked out and need to be aware that failure to do so will be interpreted as that they are undertaking personal use during the paid time and service of the Council. In addition private emails must be sent with the relevant disclaimer.**

- Where GCSx email is available to connect the sender and receiver of the email message, this should be used for all external email use and must be used for communicating PROTECT and RESTRICTED material.
- Automatic forwarding of email must be considered carefully to prevent PROTECT and RESTRICTED material being forwarded inappropriately.