MEMBERS INTERESTS 2012

A Member with a disclosable pecuniary interest in any matter considered at a meeting must disclose the interest to the meeting at which they are present, except where it has been entered on the Register.

A Member with a non pecuniary or pecuniary interest in any business of the Council must disclose the existence and nature of that interest at commencement of consideration or when the interest becomes apparent.

Where sensitive information relating to an interest is not registered in the register, you must indicate that you have an interest, but need not disclose the sensitive information.

Please tick relevant boxes

	General		Notes
1.	I have a disclosable pecuniary interest.	☐	*You cannot speak or vote and must withdraw unless you have also ticked 5 below*
2.	I have a non-pecuniary interest.	☐	*You may speak and vote*
3.	I have a pecuniary interest **because** it affects my financial position or the financial position of a person or body described in 10.1(1)(i) and (ii) **and** 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 my judgement of the public interest or it relates to the determining of any approval consent, licence, permission or registration in relation to me or any person or body described in 10.1(1)(i) and (ii) **and** 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 my judgement of the public interest	☐ ☐	*You cannot speak or vote and must withdraw unless you have also ticked 5 or 6 below* *You cannot speak or vote and must withdraw unless you have also ticked 5 or 6 below*
4.	I have a disclosable pecuniary interest (Dispensation 16/7/12) or a pecuniary interest but it relates to the functions of my Council in respect of:		
(i)	Housing where I am a tenant of the Council, and those functions do not relate particularly to my tenancy or lease.	☐	*You may speak and vote*
(ii)	school meals, or school transport and travelling expenses where I am a parent or guardian of a child in full time education, or are a parent governor of a school, and it does not relate particularly to the school which the child attends.	☐	You may speak and vote
(iii)	Statutory sick pay where I am in receipt or entitled to receipt of such pay.	☐	*You may speak and vote*
(iv)	An allowance, payment or indemnity given to Members	☐	*You may speak and vote*
(v)	Any ceremonial honour given to Members	☐	*You may speak and vote*
(vi)	Setting Council tax or a precept under the LGFA 1992	☐	*You may speak and vote*
5.	A Standards Committee dispensation applies.	☐	*See the terms of the dispensation*
6.	I have a pecuniary interest in the business but I can attend to make representations, answer questions or give evidence as the public are also allowed to attend the meeting for the same purpose	☐	*You may speak but must leave the room once you have finished and cannot vote*

'disclosable pecuniary interest' (DPI) means an interest of a description specified below which is your interest, your spouse's or civil partner's or the interest of somebody who you are living with as a husband or wife, or as if you were civil partners and you are aware that that other person has the interest.

Interest	***Prescribed description***
Employment, office, trade, profession or vocation	Any employment, office, trade, profession or vocation carried on for profit or gain.
Sponsorship	Any payment or provision of any other financial benefit (other than from the relevant authority) made or provided within the relevant period in respect of any expenses incurred by M in carrying out duties as a member, or towards the election expenses of M.

	This includes any payment or financial benefit from a trade union within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992.
Contracts	Any contract which is made between the relevant person (or a body in which the relevant person has a beneficial interest) and the relevant authority— (a) under which goods or services are to be provided or works are to be executed; and (b) which has not been fully discharged.
Land	Any beneficial interest in land which is within the area of the relevant authority.
Licences	Any licence (alone or jointly with others) to occupy land in the area of the relevant authority for a month or longer.
Corporate tenancies	Any tenancy where (to M's knowledge)— (a) the landlord is the relevant authority; and (b) the tenant is a body in which the relevant person has a beneficial interest.
Securities	Any beneficial interest in securities of a body where— (a) that body (to M's knowledge) has a place of business or land in the area of the relevant authority; and (b) either— (i) the total nominal value of the securities exceeds £25,000 or one hundredth of the total issued share capital of that body; or (ii) if the share capital of that body is of more than one class, the total nominal value of the shares of any one class in which the relevant person has a beneficial interest exceeds one hundredth of the total issued share capital of that class.

"body in which the relevant person has a beneficial interest" means a firm in which the relevant person is a partner or a body corporate of which the relevant person is a director, or in the securities of which the relevant person has a beneficial interest; "director" includes a member of the committee of management of an industrial and provident society;

"land" excludes an easement, servitude, interest or right in or over land which does not carry with it a right for the relevant person (alone or jointly with another) to occupy the land or to receive income; "M" means a member of a relevant authority;

"member" includes a co-opted member; "relevant authority" means the authority of which M is a member;

"relevant period" means the period of 12 months ending with the day on which M gives notice to the Monitoring Officer of a DPI; "relevant person" means M or M's spouse or civil partner, a person with whom M is living as husband or wife or a person with whom M is living as if they were civil partners;

"securities" means shares, debentures, debenture stock, loan stock, bonds, units of a collective investment scheme within the meaning of the Financial Services and Markets Act 2000 and other securities of any description, other than money deposited with a building society.

'non pecuniary interest' means interests falling within the following descriptions:

10.1(1)(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 (a) exercising functions of a public nature; (b) directed to charitable purposes; or (c) 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 easement, servitude, interest or right in or over land which does not carry with it a right for you (alone or jointly with another) to occupy the land or to receive income.

10.2(2) 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 connected person to a greater extent than the majority of other council tax payers, ratepayers or inhabitants of the ward, as the case may be, affected by the decision.

'a connected person' means

(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 10.1(1)(i) or (ii).

'body exercising functions of a public nature' means

Regional and local development agencies, other government agencies, other Councils, public health bodies, council-owned companies exercising public functions, arms length management organisations carrying out housing functions on behalf of your authority, school governing bodies.

A Member with a personal interest who has made an executive decision in relation to that matter must ensure any written statement of that decision records the existence and nature of that interest.

NB Section 21(13) of the LGA 2000 overrides any Code provisions to oblige an executive member to attend an overview and scrutiny meeting to answer questions.

AUDIT AND GOVERNANCE COMMITTEE **HELD:** **25 SEPTEMBER 2012**
Start: 7.00 p.m.
Finish: 8.20 p.m.

PRESENT:

Councillors: Pope (Chairman)
Forshaw (Vice-Chairman)

Councillors:

Cheetham	G. Hodson
Dereli	G.Jones
Gagen	Pendleton
Griffiths	Westley

Officers: Borough Solicitor (Mr. T. Broderick)
Borough Treasurer (Mr M Taylor)
Audit Manager (Mr. M. Coysh)
Assistant Member Services Manager (Mrs. J. Denning)

In attendance: Councillor Hennessy
Clare Degan (Audit Commission)
Paul Thompson (Audit Commission)

11. APOLOGIES

Apologies for absence were received from Councillor Pryce-Roberts.

12. MEMBERSHIP OF THE COMMITTEE

In accordance with Council Procedure Rule 4, Members noted the termination of Councillor Grant and the appointment of Councillor Griffiths for this meeting only, thereby giving effect to the wishes of the Political Groups.

13. DECLARATIONS OF INTEREST

Councillor Westley declared a non-pecuniary interest in respect of agenda item no. 5, the Audit Commission Annual Governance Report and Statement of Accounts, as a Member of Lancashire County Council and Chairman of the LCC Pension Fund.

14. MINUTES

RESOLVED: That the minutes of the meeting of the Committee held on 26 June 2012 be received as a correct record and signed by the Chairman.

15. AUDIT COMMISSION ANNUAL GOVERNANCE REPORT AND STATEMENT OF ACCOUNTS

Consideration was given to the report of the Borough Treasurer, as contained on pages 89 to 118 of the Book of Reports which provided details of the Annual Governance Report from the External Auditors and sought approval of the Statement of Accounts.

The Committee was advised that this would be the last Governance report produced by the Audit Commission due to Grant Thornton taking over the external audit function from 1 September 2012 with a saving of £42,000.

The Audit Commission referred to the recommendation in Appendix 1 in respect of declaration of interests for "key management personnel."

Comments and questions were raised in respect of the following:-

- Value For Money Studies
- Valuation of Housing Stock
- Insurances and future liabilities
- Charges for responding to correspondence from members of the public.

RESOLVED: A. That the Audit Commission's Annual Governance Report set out in Appendix 1 to the report be noted.

B. That the Accounts be approved in accordance with the relevant Accounts and Audit Regulations.

C. That the Letter of Representation set out in Appendix 2 to the report be approved.

16. INTERNAL AUDIT ACTIVITY APRIL TO SEPTEMBER 2012

Consideration was given to the report of the Borough Treasurer as contained on pages 119 to 124 of the Book of Reports which reported on the progress made against the 2012/13 Audit Plan to date.

Comments and questions were raised in respect of the following:-

- Vacancy Appointments
- Electronic Ordering
- New payroll arrangements
- Reduction in agency staff and short term contracts
- Monitoring of the Audit Plan

RESOLVED: That members noted the progress made in the year.

17. REGULATION OF INVESTIGATORY POWERS ACT QUARTERLY MONITORING OF USE OF POWERS

Consideration was given to the report of the Borough Solicitor as contained on pages 125 to 128 of the Book of Reports, the purpose of which was to monitor on a quarterly basis the use of the Regulation of Investigatory Powers Act 2000 (RIPA) to ensure it is being used consistently with the Council's Policy.

RESOLVED: A. That the Council's RIPA activity be noted.

B. That it be noted that the procedure for applying for authorisations to carry out directed surveillance and for the use of Covert Human Intelligence Sources will change from 1 November 2012.

18. DATA QUALITY PROTOCOL

Consideration was given to the report of the Transformation Manager as contained on pages 129 to 138 of the Book of Reports, the purpose of which was to update members regarding issues at a national level affecting data quality management within the Council and to approve a local Data Quality Protocol.

RESOLVED: A. That the Data Quality Protocol attached to the report be endorsed as a replacement Data Quality Strategy.

B. That regular reports relating to the superseded Data Quality Strategy be removed from the Audit and Governance Work Programme.

C. That the Transformation Manager be requested to submitted a report to a future meeting on the effectiveness of the Protocol and the Committee's Work Programme be amended accordingly.

19. REVIEW OF FRAUD, BRIBERY AND CORRUPTION ISSUES

Consideration was given to the report of the Borough Treasurer as contained on pages 139 to 170 of the Book of Reports which provided a summary of the fraud, bribery and corruption issues facing the Council and the action being taken to deal with them.

RESOLVED: A. That the updated Anti Fraud, Bribery and Corruption Policy as set out in Appendix 1 of the report be endorsed for agreement under delegated authority.

B. That the self assessment of Fraud and Corruption issues as set out in Appendix 2 of the report be noted.

C. That the Counter Fraud Plan as set out in Appendix 3 to the report be endorsed.

20. AUDIT & GOVERNANCE COMMITTEE WORK PROGRAMME

Consideration was given to the Committee's programme of work, as contained on page 171 of the Book of Reports.

RESOLVED: That the work programme be amended as follows:

A. That the training session in September 2013 be Housing-Self financing.

B. That "the effectiveness of the Data Quality Protocol" be included in the September 2013 meeting.

C. That “a basic guide to Governance” be provided at a future training session.

- CHAIRMAN -

AGENDA ITEM: 5

AUDIT AND GOVERNANCE COMMITTEE:

29 January 2013

Report of: Borough Treasurer

Relevant Managing Director: Managing Director (People and Places)

Contact for further information: Natasha Bryan (Extn. 5098)
(E-mail: natasha.bryan@westlancs.gov.uk)

SUBJECT: RISK MANAGEMENT FRAMEWORK

Wards affected: Borough wide

1.0 PURPOSE OF THE REPORT

1.1 To set out details of the operation of the Risk Management Framework over the last twelve months and to review the Risk Management Policy.

2.0 RECOMMENDATIONS

2.1 That the continuing effective operation of the Risk Management Framework be noted.

2.2 That the proposed amendment to the Risk Management Policy set out in paragraph 4.7 be endorsed for submission to Cabinet for formal approval.

3.0 BACKGROUND

3.1 West Lancashire Borough Council continues to recognise the importance of identifying, evaluating and managing all Key and Service Risks that could affect the Council.

3.2 Risk Management covers the whole spectrum of risks and not just those associated with finance, business continuity, insurance and health and safety. It also considers risks associated with service provision, compliance with legislation, public image (reputation) and environment.

3.3 Risk management is not about being 'risk averse' – it is about being 'risk aware'. Risk is ever present and some amount of risk taking is inevitable if the Council is

to achieve its objectives. Risk Management is about effectively managing risks that could affect the Council. It is also about making the most of opportunities and achieving objectives. By being 'risk aware' the Council is in a better position to avoid threats and take advantage of opportunities.

3.4 The terms of reference of the Audit and Governance Committee include monitoring the effectiveness of the Risk Management Framework and corporate governance processes within the Council. This report assesses the operation of the Risk Management Framework over the last twelve months and the main developments that have occurred during that time.

4.0 DEVELOPMENTS OVER THE LAST TWELVE MONTHS

4.1 During the course of the year an Internal Audit review was conducted over the use of Covalent (the Council's Performance Management System) for managing and reporting on Service risks and Service Risk Registers. This audit concluded that in general risks were effectively identified from service business plans and that there was a logical link between the risks recorded and published priorities. It also found that there were appropriate escalation procedures in place for the sample of risks investigated.

4.2 The audit identified a number of areas for development including improving the consistency in which Services deal with similar issues and in certain cases ensuing that the records maintained on Covalent are kept up to date. The results of the audit have been discussed at the most recent Risk Management Officer Working Group and an action plan agreed to address these issues.

4.3 In recent months work has been undertaken to prepare for the tendering of the new Insurance Contract (which is covered in more detail in a separate report elsewhere on the agenda). During this process both our current insurance provider and our brokers (AON) have considered the Council's Risk Management Framework and assessed it to be robust. This is important because the insurance premiums that will be charged will take into account whether the Council has effective systems and procedures in place. Risk Management has become even more important within the current climate where there is a potential for increased premiums in a market that our Brokers have advised is hardening.

4.4 As part of our approach to reducing risks from an insurance perspective, meetings have been taking place with Services to consider higher risk areas such as Housing and Regeneration in relation to commercial buildings, and Street Scene in relation to motor vehicle accidents.

4.5 This has resulted in a working group being established within Street Scene to consider incidents and to identify what risk management processes can be put in place to reduce insurance claims. The group is in the process of establishing its terms of reference and membership, but it is proposed that the first meeting will take place in late January. Already such initiatives as driver reassessments, refreshed risk assessments and new items to be included in the current tool box talks have been introduced. Similar processes are underway in other service areas.

4.6 Risk Management training has been held for Officers within several Services and further training is propsed to take place over the coming months. The scheduled meetings of the Risk Management Officer Working Group have also taken place over the year.

.

4.7 The Risk Management Policy has been reviewed and continues to meet best practice requirements. Consequently only one change is proposed to the Policy, which is to change the frequency of producing monitoring reports on Service Risk Registers for Heads of Service from a quarterly to a six monthly basis. This will then be consistent with the reporting frequency of risk management reports to Cabinet and the frequency of Risk Management Officer Working Group meetings.

5.0 REVIEW OF EFFECTIVENESS

5.1 The Risk Management Framework has once again operated effectively over the last year. The arrangements in place include the Key and Service Risk Registers, a Risk Management Policy, a Risk Management work programme and a training programme for Members and Officer. The Risk Registers continue to be maintained on line and are subject to regular review and updating.

6.0 RISK ASSESSMENT

6.1 The continued review of the Risk Management Framework is essential to ensure the successful achievement of the Authority's objectives, demonstrate effective provision of its services and the maximisation of opportunities. If we are unable to maintain an effective Risk Management Framework, we could endanger the achievement of our primary objectives. By continually monitoring and reviewing the Authority's Risk Management Framework it should continue to improve, develop and meet best practice requirements.

Background Documents

There are no background documents (as defined in section 100D(5) of the Local Government Act 1972) to this report.

Equality Impact Assessment

The decision does not have a direct impact on members of the public, employees, elected members and / or stakeholders. Therefore no Equality Impact Assessment is required.

Appendices

None

AGENDA ITEM: 6

AUDIT AND GOVERNANCE COMMITTEE:

29 January 2013

Report of: Borough Treasurer

Relevant Managing Director: Managing Director (People and Places)

Contact for further information: Mr M.Coysh (Extn. 2603)
(E-mail: mike.coysh@westlancs.gov.uk)

SUBJECT: INTERNAL AUDIT ACTIVITY APRIL TO DECEMBER 2012

Wards affected: Borough wide

1.0 PURPOSE OF THE REPORT

1.1 To report progress against the 2012/13 Audit Plan to date.

2.0 RECOMMENDATION

2.1 That Members note progress in the year to date and direct any questions to the Internal Audit Manager who will be present at the meeting.

3.0 BACKGROUND

3.1 This Committee approved the 2012/13 Internal Audit Plan and resolved that a written report be brought back quarterly to enable progress against it to be monitored.

4.0 INTERNAL AUDIT ACTIVITY TO DATE

4.1 A report summarising progress in the first three quarters is attached and the Internal Audit Manager will be present to answer questions in relation to it.

4.2 This work will inform the overall opinion relating to the system of internal control in the Internal Audit Annual Report.

4.3 There are no significant issues arising from Internal Audit's work in the period covered by this report that would merit being drawn specifically to the attention of

Audit and Governance Committee in advance of my annual report. The Data Management audit has helped to identify a number of areas for development and these issues are covered in the Information governance / Data Protection report elsewhere on the agenda.

5.0 RESOURCE ISSUES

5.1 Since the last report approval has been given to fill a vacancy in the section on a temporary basis. While the reduced resources available in the section early in the year have had an impact on the work of the section to date, satisfactory progress is now being made and it is anticipated that the plan will be substantially complete by the end of the financial year.

6.0 SUSTAINABILITY IMPLICATIONS/COMMUNITY STRATEGY

6.1 There are no significant sustainability impacts associated with this report and, in particular, no significant impact on crime and disorder. The report has no significant links with the Sustainable Community Strategy.

7.0 FINANCIAL AND RESOURCE IMPLICATIONS

7.1 All the activity referred to in this report is covered by existing budget provisions.

8.0 RISK ASSESSMENT

8.1 This report summarises progress against Internal Audit's work programme for the year. Internal Audit activity is a key source of assurance to this Committee that risks to the Council's overall objectives are being properly managed.

Background Documents

There are no background documents (as defined in Section 100D(5) of the Local Government Act 1972) to this Report.

Equality Impact Assessment

The decision does not have any direct impact on members of the public, employees, elected members and / or stakeholders. Therefore no Equality Impact Assessment is required.

Appendices

1. Internal Audit third quarter update report.

APPENDIX

Audit and Governance Committee January 2013.

Internal Audit Update Report 2012/13 to date

Progress against the Plan

Title	Position
Annual Governance Statement	Ongoing activity
Shared and Contracted Services	Ongoing activity
MSR and OR implementation	Limited work undertaken to date
Data Management	Work Complete
ICT	Review of contract implementation
Matrix	Work Complete
Human Resources	Limited work undertaken to date
Performance Management	Work in progress
Corporate Health and Safety	Work in progress
Business continuity	Work Complete
Contract Audit	Ongoing activity
QL Procurement	Work Complete
Procurement through Official Order	Work in progress
Benefits	Limited work undertaken to date
Council Tax	Work in progress
NNDR	Work not commenced
Debtors	Work in progress
Creditors	Work not commenced
Right to Buy / Housing Act Advances	Work not commenced
Accounting Controls	Work not commenced
Payroll	Work Complete
Rents	Work in progress
Treasury Management	Work not commenced
Fees and Charges	Work not commenced
Housing Stock Maintenance	Work in progress
Q.L (Housing Management system)	Work in progress
Cash to Leave and Transfer Incentive Schemes	Work in progress
Licensing	Work in progress
Depot	Work not commenced
Transport	Review of contract implementation
Community Safety CCTV	Work not commenced
Leisure	Review of contract implementation
Customer Services	Work Complete
Strategic Asset Management Plan	Limited work undertaken to date
Building Control	Work Complete
Estates and Valuation	Work not commenced
National Fraud Initiative	Ongoing activity
Money Laundering Controls	Ongoing activity
Anti Fraud and Corruption Policy and Action Plan	Work Complete

Summary	
Work Complete	8
Audits in progress	10
Ongoing activities	5
Reviews of contract implementation	3
Limited work undertaken to date	4
Work not yet commenced	9
Total	**39**

At the end of the third quarter 26 out of 39 items (67%) were either in progress or completed.

Notable matters

Payroll

The previous update report identified new payroll arrangements following the expiry of the licence with our previous software provider at the end of October as a key issue. Due to the timescales involved examination of the new arrangements took place as they developed and migration to the new systems was completed in November. The arrangements are now in operation and the transition took place with minimal disruption to payment routines. Further work will need to be undertaken in the future in relation to controls on payroll as part of the regular audit review of this system.

Data Management

This year's audit plan included a scheduled exercise on data management activities which was completed in December. Recommendations for enhancements to the Council's existing control framework arising from that review are being incorporated into the measures identified in the report on Information Governance and Data Protection which appears elsewhere on this agenda.

Revenues and Benefits

It was agreed with LCC / OCL that internal Audit work on the majority of systems under their control would take place following the planned move of Revenues, Benefits and ICT staff to the new facility at Lancashire Place. The move was postponed by LCC / OCL and while it has now been completed system migrations from existing WLBC platforms to One Connect Ltd systems are now underway. Internal audit are receiving training on these and will be in a position to review the new systems as they come on stream. Audits of Council Tax and Debtors are currently in progress.

Investigations

There are no formal investigations in progress at this time

Progress on significant governance issues identified in the last Annual Governance Statement.

The key issue identified in the Annual Governance Statement was the scale of the financial challenges facing the Council and a key control measure relating to this was the Councils Business Plan. The Major Service Review process has been a keystone of the Business Plan and has enabled the Council to find significant savings without recourse to draconian cuts in front line services.

Summary

A report of progress against the Internal Audit Plan is brought to each meeting of Audit and Governance Committee. This report covers the period to the end the third quarter based on information available when the report was drawn up.

During this period 165 days had been lost to a vacancy. Progress against the plan to date has inevitably been affected but resources have been secured for completion of the remainder of the plan.

Indications at this time are that by the end of the financial year sufficient work will have been undertaken to enable a valid judgement to be made on the operation of the control environment.

Management have agreed action plans to secure improvement in relation to any issues identified by work completed against the plan to date.

AGENDA ITEM: 7

AUDIT AND GOVERNANCE COMMITTEE: 29 JANUARY 2013

Report of: Borough Solicitor

Relevant Managing Director: Managing Director (People and Places)

Contact for further information: Mr T P Broderick (Ext 5001)
(E-mail: terry.broderick@westlancs.gov.uk)

SUBJECT: REGULATION OF INVESTIGATORY POWERS ACT – QUARTERLY MONITORING OF USE OF POWERS

Borough Wide Interest

1.0 PURPOSE OF THE REPORT

1.1 To monitor on a quarterly basis the use of the Regulation of Investigatory Powers Act 2000 (RIPA) to ensure it is being used consistently with the Council's Policy.

2.0 RECOMMENDATIONS

2.1 That the Council's RIPA activity be noted.

3.0 BACKGROUND

3.1 The Council employ a number of investigative techniques including surveillance, which assist its regulatory functions. Relevant areas of activity can potentially include investigation by Internal Audit, Benefits Fraud Team, Environmental Health, Housing, Licensing, CCTV Services and the MAPs Team. Some activities must be undertaken in accordance with the Regulation of Investigatory Powers Act 2000 ("RIPA"). RIPA, its subordinate legislation and Codes of Practice prescribe the type of activities permitted and the procedures required to monitor RIPA activity within the Council. As reported previously, this is now supplemented by monitoring through this Committee.

3.2 In accordance with the current Scheme of Delegation the Joint Managing Directors and Heads of Service consider whether or not to grant authorisations for surveillance activity. In practice under the Policy this is restricted to the Joint Managing Directors, the Assistant Director (Community Services) and the Assistant Director (Housing and Regeneration). In the case of the authorisation

of communications data (i.e. relating to material, such as subscriber and billing records obtained from telecommunications service providers, but not the content of the communication) the authorisation must be from the Joint Managing Directors and via the externally approved specially trained officer (SPOC).

3.3 The Council's approved RIPA Guide is made available on the Council's Intranet and is a working document to assist investigating and co-ordinating officers within the Council. The Guide stresses that grantors must believe the authorised activity is (1) necessary for preventing and detecting crime (the criminal offence which is sought to be prevented or detected is to be punishable, whether on summary conviction or on indictment, by a maximum term of at least six months' imprisonment, or would constitute an offence involving the sale of tobacco and alcohol to underage children) and (2) is proportionate to what is sought to be achieved in carrying out the surveillance activity. If it fails either test, authorisations should not be granted. The RIPA Guide has been updated to reflect recent legislative changes reported to the last meeting.

3.4 The Code requires that Councillors should consider internal reports on the use of RIPA on at least a quarterly basis to ensure that it is being used consistently with the Council's Policy and that the Policy remains fit for purpose. It continues that Councillors should not, however, be involved in making decisions on specific authorisations. It is stressed that the involvement of elected members is not to extend to operational decision making or stipulate in detail how the Council discharges the procedure. The Government's position is that there should be no possibility of political interference in law enforcement operations.

4.0 MONITORING OF RIPA ACTIVITY

4.1 In the last quarter no covert surveillance has been authorised.

4.2 The Senior Responsible Officer proactively seeks to ensure that the use of covert surveillance in this authority is well regulated. Applications for authorisation to use covert surveillance must be rejected when the Authorising Officer is not satisfied that the surveillance is necessary or proportionate and legal advice should be sought by Authorising Officers in appropriate cases.

4.3 Amongst other matters, a RIPA guidance note is circulated within the Council at regular intervals.

5.0 THE RIPA POLICY

5.1 The RIPA Guide is annually approved by Cabinet; it is important to ensure the use of RIPA is consistent with the Council's policy.

6.0 SUSTAINABILITY IMPLICATIONS/COMMUNITY STRATEGY

6.1 There are no significant sustainability impacts associated with this report and, in particular, no significant impact on crime and disorder. The report has no significant links with the Sustainable Community Strategy.

7.0 FINANCE AND RESOURCE IMPLICATIONS

7.1 There are no additional significant financial and resource implications arising from this report.

8.0 RISK ASSESSMENT

8.1 The Council could be in breach of the relevant legislation if it does not follow the procedures set out in the RIPA Orders and Codes. This could result in the inadmissibility of evidence and the possibility of breaches of the Human Rights Act 1990.

Background Documents

There are no background documents (as defined in Section 100D(5) of the Local Government Act 1972) to this report.

Equality Impact Assessment

This will be considered in relation to any particular authorisation.

Appendix

None

AGENDA ITEM: 8

AUDIT AND GOVERNANCE COMMITTEE:

29 January 2013

Report of: Borough Treasurer

Relevant Managing Director: Managing Director (People and Places)

Contact for further information: Mr M.Coysh (Extn. 2603)
(E-mail: mike.coysh@westlancs.gov.uk)

SUBJECT: INTERNAL AUDIT CHARTER

Wards affected: Borough wide

1.0 PURPOSE OF THE REPORT

1.1 To consider proposals for a new Internal Audit Charter.

2.0 RECOMMENDATION

2.1 That the Audit Charter attached at appendix 1 be approved to take effect from 1/4/2013

3.0 BACKGROUND

3.1 The Code of Practice for Internal Audit in Local Government in the United Kingdom 2006 (The Code) requires Internal Audit's terms of reference to be formally approved by the authority and in West Lancashire this has been achieved by incorporating them into an Internal Audit Charter.

3.2 The Terms of reference of this Committee include approval of the Internal Audit Charter. The current Charter was adopted some years ago and it now requires updating to reflect changes which have taken place in the authority since it was drawn up.

4.0 CURRENT POSITION

4.1 The Internal Audit Charter forms part of the framework which demonstrates compliance with The Code thereby discharging the Authority's statutory duty to

maintain an adequate and effective system of internal audit of its accounting records and system of internal control.

4.2 The Charter is a key document which:

- supports the organisational independence of Internal Audit
- sets out Internal Audit's remit
- defines Internal Audit's reporting lines

4.3 The proposed Charter has been substantially redrafted to make it clearer and easier to read than its predecessor, bring it into line with current committee arrangements, management structures and job titles and reflect changes to Internal Audit's remit following service restructuring. For comparative purposes the existing Internal Audit Charter has also been included as an appendix to this report.

5.0 SUSTAINABILITY IMPLICATIONS/COMMUNITY STRATEGY

5.1 There are no significant sustainability impacts associated with this report and, in particular, no significant impact on crime and disorder. The report has no significant links with the Sustainable Community Strategy.

6.0 FINANCIAL AND RESOURCE IMPLICATIONS

6.1 All the proposals in this report are covered by existing budget provisions.

7.0 RISK ASSESSMENT

7.1 The formal approval of terms of reference for Internal Audit is required for compliance with the Code of Practice for Internal Audit in Local Government in the United Kingdom 2006. This Internal Audit Charter contains Internal Audit's terms of reference. Approval of the Charter is a key step in ensuring that the Council can demonstrate compliance with one of its statutory obligations.

Background Documents

There are no background documents (as defined in Section 100D(5) of the Local Government Act 1972) to this Report.

Equality Impact Assessment

The decision does not have any direct impact on members of the public, employees, elected members and / or stakeholders. Therefore no Equality Impact Assessment is required.

Appendices

1. Proposed new Internal Audit Charter

2. Existing Internal Audit charter

APPENDIX 1

WEST LANCASHIRE BOROUGH COUNCIL
INTERNAL AUDIT CHARTER

INTRODUCTION

Internal Audit is an independent review function set up within the organisation to provide a service to the Council and all levels of management. The Audit Manager is responsible for the review of all aspects of risk management and control throughout the Council's activities.

The existence of Internal Audit does not diminish the responsibility of management to establish adequate systems of internal control to ensure that activities are conducted in a secure, efficient and well-ordered manner in accordance with the Scheme of Delegation and Financial Regulations.

INDEPENDENCE

Internal Audit is independent of the activities which it audits to enable it to provide the objective and unbiased judgements essential to the impartial advice and assurance it provides to management.

To ensure this Internal Audit operates in a framework that allows:

- segregation from line operations
- unrestricted access to senior management
- reporting in its own name

.

Every effort will be made to preserve its objectivity by ensuring that all auditors are free from any conflicts of interest and do not undertake non-audit duties, unless they have been specifically considered and agreed by the Audit Manager.

ROLE AND SCOPE OF INTERNAL AUDIT

The role of Internal Audit is to assess the Council's key risks, evaluate the adequacy and effectiveness of the system of risk management and internal control, and to recommend where and how improvements can be made.

The main functions of Internal Audit are to review, appraise and report on:

(a) the adequacy and effectiveness of the systems of financial, operational and management control and their operation in practice in relation to the business risks to be addressed;

(b) the extent of compliance with, relevance of and financial effect of policies, standards, plans and procedures established by the Council and the extent of compliance with external laws and regulations, including reporting requirements of regulatory bodies;

(c) the extent to which assets and interests are acquired economically, used efficiently, accounted for and safeguarded from losses of all kinds arising from waste, extravagance, inefficient administration, poor value for money, fraud or other cause and that adequate business continuity plans exist;

(d) the suitability, accuracy, reliability and integrity of financial and other management information and the means used to identify, measure, classify and report such information;

(e) the integrity of processes and systems, including those under development, to ensure that controls offer adequate protection against error, fraud and loss of all kinds; and that the process aligns with the organisation's strategic goals;

(f) the suitability of the organisation of the units audited for carrying out their functions, and to ensure that services are provided in a way which is economical, efficient and effective;

(g) the follow-up action taken to remedy weaknesses identified by Internal Audit review, ensuring that good practice is identified and communicated widely;

(h) the operation of the organisation's corporate governance arrangements;

Internal Audit, therefore, has unrestricted access to all of the authority's activities and unrestricted access to all records and assets it requires.

Internal Audit, through the Audit Manager, where he deems necessary, will have unrestricted access to: The Managing Directors, Members, Heads of Services and all Authority employees and contractors.

INTERNAL AUDIT RESPONSIBILITY

The Audit Manager will be required to manage the provision of a complete Audit Service to the Authority in addition to the investigation of fraud where required. In discharge of this duty, the Audit Manager will:

- prepare a rolling five-year strategic risk-based audit plan in consultation with Heads of Service. This strategic plan will be regarded as flexible rather than as an immutable expression of audit policy

- translate the strategic plan into annual plans based on the significant risks to which the Council is exposed for presentation to the Audit and Governance Committee for agreement

- ensure a system of close supervision of audit work, and maintain a review of audit files through the supervisory structure

- carry out a continuous review of the development and training needs of all Audit Personnel and arrange, where appropriate, training to maintain a professional audit staff.

- ensure that all work is carried out in accordance with the relevant professional standards.

- prepare, for agreement with the Managing Directors and Borough Treasurer, annual reports on audit activity for presentation to the Audit and Governance Committee.

Internal Audit will liaise with the Council's External Auditors in order to optimise audit coverage from available resources.

Internal Audit investigate fraud and irregularities in accordance with Council policies and procedures.

Internal Audit may also carry out exercises in conjunction with other bodies such as other Local Authorities, the Police and the HM Revenue and Customs etc.

AUDIT REPORTING

Internal audit reports regularly to management on the results of audit work which provides them with regular assessments of the adequacy and effectiveness of their systems of risk management and internal control.

In addition to this the Audit Manager has access to and may report directly to any officers and members, particularly those charged with governance.

Internal audit regularly reports the results of its work to the Audit and Governance Committee in relation to:

- regular assessments of the adequacy and effectiveness of the Council's systems of risk management and internal control based on the work of internal audit
- progress against the annual Internal Audit Plan
- the adequacy of its resources for maintaining adequate audit coverage in accordance with statute.

RELATED DOCUMENTS

This document is one of a series that, together, constitute the policies of the Authority in relation to anti-fraud, bribery and corruption. The other documents include:

Anti-Fraud, Bribery and Corruption Policy

Whistleblowing Code

Anti-Money Laundering Policy

Officers Code of Conduct

Disciplinary Procedures

APPENDIX 2

INTERNAL AUDIT CHARTER

Introduction

The main determinant of the effectiveness of Internal Audit is that it is seen to be independent. To ensure this, Internal Audit will operate within a framework that allows:

- unrestricted access to senior management
- reporting in its own name
- segregation from line operations.

Every effort will be made to preserve objectivity by ensuring that all audit members of staff are free from any conflicts of interest and do not undertake any non-audit duties*, with the exception of exigencies of the service agreed by the Audit Manager.*

All Internal Audit activity is carried out in accordance with financial regulations and procedures.

The existence of Internal Audit does not diminish the responsibility of management to establish systems of internal control to ensure that activities are conducted in a secure, efficient and well-ordered manner.

Objectives of Internal Audit

As an independent appraisal function within the authority, the primary objective of Internal Audit is to review, appraise and report upon the adequacy of internal controls as a contribution to the proper, economic, efficient and effective use of resources. In addition, the other objectives of the function are to:

Support the Executive Manager Financial Services to discharge duties as Proper Officer

Contribute to and support the financial services division's objective of ensuring the provision of, and promoting the need for, sound financial systems

Support the corporate Comprehensive Performance Assessment (and Best Value?) processes.

Provide a quality fraud investigation service which safeguards public money

Scope of Internal Audit

The scope of Internal Audit allows for unrestricted coverage of the authority's activities and unrestricted access to all records and assets deemed necessary in the course of the audit.

Internal Audit, through the Audit Manager, where he deems necessary, will have unrestricted access to:

The Chief Executive

Members

Individual Chief Officers

All Authority Employees.

Location of Internal Audit

Internal Audit is located within the Finance Department in accordance with the Financial Regulations, under the direction of the Proper Officer, Executive Manager Financial Services.

Internal Audit Responsibility

The main areas of Internal Audit responsibility within the Authority are to:

1. Review, appraise and report on:

- the extent to which its assets and interests are accounted for and safeguarded from loss
- the soundness, adequacy and application of internal controls
- the suitability and reliability of financial and other management data, including aspects of performance measurement.

2. Support the Best Value process by participation in any corporate and divisional reviews as appropriate and in any VFM exercises as required

3. Investigate fraud and irregularities in accordance with Council procedures.

(With the exception of those elements of Housing Benefit/Council Tax Benefit Fraud specifically delegated to the Council's Benefit Inspection Team).

4. Advise on internal control implications of new systems.

5. Support the corporate risk management function.

Audit Style and Content

The primary task of Internal Audit is to review the systems of internal control operating throughout the Authority, and for this purpose it will adopt a predominantly systems-based approach to Audit.

The Audit Manager will be required to manage the provision of a complete Audit Service to the Authority which will include systems, regularity, computer and contract audit in addition to the investigation of fraud. In discharge of this duty, the Audit Manager will:

- prepare a rolling five-year strategic risk-based audit plan in consultation with Departmental Senior Management, for formal ratification by the Executive Manager Financial Services. This strategic plan will be regarded as flexible rather than as an immutable expression of audit policy

- translate the strategic plan into annual plans for formal agreement with the Executive Manager Financial Services

- ensure a system of close supervision of audit work, and maintain a review of audit files through the supervisory structure

- ensure that all work is carried out in accordance with the relevant professional standards.

- liase with the Benefit Inspection Team (whose remit is to investigate claimant and landlord fraud specifically in relation to Housing and Council Tax Benefits). The purpose of this liaison is to enable the Audit Manager to maintain corporate intelligence about trends in fraudulent activity. Internal Audit may also carry out joint exercises involving Benefit Inspection Team Members where appropriate.

- prepare, for agreement with the Chief Executive and Executive Manager Financial Services, annual reports on audit activity for presentation to the Authority.

In order to establish an audit presence and to create sound informal lines of communication, as much audit work as possible will be done on location.

Internal Audit testing may go beyond the records and adopt a more ‘physical’ approach.

Audit Resources

As far as is practicable, Internal Audit will not participate in the day-to-day operation of any systems of internal financial control. However, in strict emergency situations only, audit personnel may be called upon to carry out non-audit work on a short-term basis with the agreement of the Audit Manager.

Members of the Internal Audit Section will be expected to contribute to the general management and conduct of business through membership of working groups and participation in ad hoc exercises with the agreement of the Audit Manager.

Upon request from the *Executive Manager Financial Services*, appropriate specialists from departments other than Finance should be made available to take part in any audit, VFM, Best Value or CPA Review requiring specialist knowledge.

Internal Audit will liaise with the Council's External Auditors in order to optimise audit coverage from available resources.

Internal Audit may also carry out exercises in conjunction with other bodies such as other Local Authorities, the Audit Commission, the Police and the Inland Revenue etc.

Audit Training

The Audit Manager will carry out a continuous review of the development and training needs of all Audit Personnel and will arrange in-service training covering both internal and external courses.

This will cover generic, professional and technical training, specific auditing techniques and specialist areas in order to maintain an appropriate mix of skills within the section.

Audit Reporting

Audit assignments will be the subject of formal reports. Draft reports will be sent to the Managers responsible for the area under review for agreement to the factual accuracy of findings

All Internal Audit Reports will normally be treated as confidential to unless alternative arrangements have been expressly made with the management concerned except as follows. The Audit Manager reserves the right to copy reports to the Chief Executive, the Section 151 Officer, the Monitoring Officer, the Standards Committee or the Authority's External Auditors or other appropriate external agencies as he deems appropriate.

Related Documents

This document is one of a series that, together, constitute the policies of the Authority in relation to anti-fraud and corruption. The other documents are:

Anti-Fraud and Corruption Policy

Whistle-Blowing Policy

Benefits Fraud Prosecution Policy

Benefits (Verification Framework) Anti Fraud Policy

Officers Code of Conduct

Disciplinary Procedures

AGENDA ITEM: 9

AUDIT AND GOVERNANCE COMMITTEE: 29th JANUARY 2013

Report of: Borough Treasurer

Relevant Managing Director: Managing Director (People and Places)

Contact for further information: Mike Kostrzewski (Extn. 5374)
(E-mail: mike.kost@westlancs.gov.uk)

SUBJECT: COUNCIL INSURANCE ARRANGEMENTS

Wards affected: Borough wide interest

1.0 PURPOSE OF THE REPORT

1.1 To provide an update on insurance issues, claims history and investigation, and the tenants home contents insurance scheme. Also, the collaborative insurance procurement process to date.

2.0 RECOMMENDATIONS

2.1 That the report be noted.

3.0 CURRENT ARRANGEMENTS

3.1 The Councils current insurers are Chartis and they have appointed Risk Management Partners (RMP) to manage the contract on their behalf. They provide insurance cover for all the main classes of insurance risk for the Council, detailed below:

	£ premium
• Employers & Public liability	83,100
• Motor	90,500
• Property	295,850
• Terrorism	13,150
• Fidelity guarantee	1,350
• Personal accident/Travel	3,940
• Contract works	13,880

3.2 The current price for the above cover is some £501,770 including insurance premium tax at 6%, as detailed above, with property cover being far the largest element of the insurance cover.

3.3 RMP engages a partner organisation, Gallagher Bassett (GB) to manage any claims that may arise at West Lancs B.C. When a claim is submitted the Insurance section will investigate the situation and if deemed appropriate set up an appropriate file and inform the claim handlers. We will look for evidence to defend the claim in order to avoid any liability falling on the Council. GB will assist us in this process and we like to have a robust mind set in repudiating such claims. Our performance indicator for settling claims at nil is regularly above 80% to 90%.

3.4 The Council utilises the services of an Insurance broker, Aon, to assist us with any insurance or risk management issues that may arise. This service entails quarterly meetings to discuss any new insurance matters that have recently arisen and we inform them of any risk management initiatives that have been implemented. Also, each year RMP require a full update on the Insurance position of the Council, covering such issues as, the value of property cover, number of employees, motor fleet numbers and so forth. Aon assist us with this compilation and liaise with RMP in order to ensure a smooth completion of the exercise. Aon also provide telephone support as matters arise.

3.5 Our relationship with both the claim handlers and our brokers is based upon a sound professional basis which is actively managed by the Insurance section. We ensure that we take the lead in making the critical decisions whilst fully researching any incidents and taking on board any advice proffered.

3.6 Our claims history was reviewed as part of a recent actuarial review and it detailed that for the last five years we had an overall loss ratio of some 50% compared to premiums paid. They stated that this is a favourable position, it must be borne in mind that some claims are 'long tail' in their nature i.e. they take some years to manifest, for example industrial deafness and insurers need to plan for such future claims.

3.7 Some of the levels of cover that the Council has in place are detailed below:

- Property £778m
- Commercial properties rent, cover for 36 months, £5.4m
- Fidelity guarantee, £1m
- Replacement IT hardware, £1.17m
- Reinstatement IT data, £1m
- Vehicles, 76 plus mowers and plant
- Employee salaries £15m

Each year these figures require updating and this will involve dealing with the Councils estates section for property matters and IT section for hardware and data issues.

3.8 The Council also operates the tenants home contents insurance scheme for our Council house occupants on behalf of Aviva. The purpose of this scheme is to

offer a low cost home contents insurance plan that has the benefits of a nil excess and one in which the premiums have not risen for the last nine years. There are approximately 17% of our Council households who have opted into the scheme. The insurers, Aviva, are complementary about the level of take up and the general operation of the scheme. We publicise the scheme by including details within the tenants handbook and a recorded message that is played by the housing repairs call centre.

3.9 The Council has varying excess levels to reflect the risk that the Council is willing to undertake. For example, combined liability (Employers and Public Liability) has an excess of £50,000, motor is £250 whilst property has various levels up to a maximum of £1,000. Also, the perils that are covered by Insurance will vary and this is partly dependant about what risks the Insurance Companies will accept. Varying excess levels will have an effect on the premiums levied by insurance companies.

4.0 INSURANCE FUND

4.1 The Council has an Insurance fund of some £2.7m and this is subject to a full actuarial review every four years and a mini review two years after a full review. This is to ensure that the fund is adequate for the actual and estimated potential insurance risks facing the Council. A full review was concluded in September 2012 covering the period to April 2012 with projections to April 2013. The report covered several areas, including the fund level, claims history, future injections to the fund and emerging claims. The main finding of the report was that the estimated fund level calculated by the actuary of £2.3m, which was a prudent calculation, is more than matched by the current fund level of £2.7m.

4.2 In the past the Council was part of an insurance organisation called Municipal Mutual Insurance, which was a collaboration of Council organisations. This organisation ceased insurance operations in 1992 and arrangements were put in place for liabilities to be met by the previously accrued asset fund, termed a scheme of arrangement. It was considered by the body overseeing the scheme that a solvent run off, whereby liabilities would be met by the assets, would be achieved. However, over recent years the financial position has deteriorated, mainly as a result of a Court case that was recently lost by the scheme administrators, this has meant that a solvent run off is now not envisaged. As such, the scheme administrator duties have passed to Ernst & Young. The implication for the Council is that it is likely to have to make payments to meet these past liabilities. The maximum liability of the Council is £0.85m, which is provided for in full in the Insurance fund. However, some observers at this stage consider that the liability could be around 25% of the maximum £850k i.e. some £200k.

5.0 COLLABORATIVE INSURANCE CONTRACT

5.1 The Council's current insurance contract ceases at the end of March 2013. Our insurance brokers had advised us that the insurance market, which had been at a low ebb for some time was now starting to harden i.e. the market prices were increasing. The soft market had benefitted us when we last went to tender in 2008 hence negotiating a rising market has required some careful consideration,

especially considering that the insurance market does not have many players in this sector.

5.2 We considered the issue with Aon and it was suggested that as they were the brokers for Pendle and Burnley Councils, that we undertake a joint procurement exercise. This would have the benefit of increasing the value of the contract and would encourage competition, which would hopefully be reflected in the tender prices submitted.

5.3 Discussions between the Councils have been very useful and professional and from an information sharing point of view, quite enlightening. This is particularly the case with regards the differing excess levels that the Councils have in place.

5.4 The procurement process that was arranged ensured that if the same insurer was appointed by more than one Council then a package discount would be applied to the price of the submitted bid. However, it was also ensured that if it was beneficial for any Council to independently appoint their own insurer, so that they were not tied in to another Council, that this facility was also an option.

5.5 Tenders have recently been received and the bids are currently being evaluated by Councils, in conjunction with their brokers. Further details will be provided to members in the coming weeks.

6.0 SUSTAINABILITY IMPLICATIONS/COMMUNITY STRATEGY

6.1 There are no significant sustainability impacts associated with this report and in particular, no significant impact on crime and disorder. The report has no significant links with the Sustainable Community Strategy.

7.0 FINANCIAL AND RESOURCE IMPLICATIONS

7.1 The current Insurance contract ceases at the end of March 2013. A collaborative insurance tender has been undertaken in order to try and obtain the best possible economic price for the new contract period. The tender outcome will only be fully known in mid February 2013.

7.2 The recent actuarial review of the insurance fund will also help to ensure that an adequate level of cover is in place.

8.0 RISK ASSESSMENT

8.1 The collaborative nature of the tender process, within which we utilised insurance brokers to assist us, is designed to ensure that we obtain the best economic price possible within a hardening market.

Background Documents

There are no background documents (as defined in Section 100D(5) of the Local Government Act 1972) to this Report.

Equality Impact Assessment

The decision does not have any direct impact on members of the public, employees, elected members and / or stakeholders. Therefore no Equality Impact Assessment is required.

Appendices

None

AGENDA ITEM: 10

AUDIT & GOVERNANCE:
29 January 2013

Report of: Borough Solicitor

Relevant Managing Director: Managing Director (People and Places)

Contact for further information: Terry Broderick – Borough Solicitor (Extn.5001)

SUBJECT: INFORMATION GOVERNANCE/DATA PROTECTION

Wards affected: Borough wide.

1.0 PURPOSE OF REPORT

1.1 To enhance information governance/data protection arrangements by clarifying/ formalising governance arrangements in line with recommended good practice.

2.0 RECOMMENDATIONS

2.1 That the delegation to the Borough Solicitor at Constitution 4.2 A, B (i) para16 be amended to read: "To co-ordinate compliance with the requirements of the data protection legislation, determine requests for disclosure of personal data and act as the Council's Senior Information Risk Owner (SIRO)".

2.2 That the updated Data Protection Policy attached as Appendix 2 be approved and it be noted that a proposal for additional resources of £30,000 will be submitted to Council in February 2013.

3.0 BACKGROUND

3.1 The Information Commissioner and the Department for Communities and Local Government promote the importance of good information governance. They draw attention to the significant change that came into force in April 2010, which enabled the Information Commissioner's Office (ICO) to order organisations to pay up to £500,000 as a penalty for serious breaches of data protection principles. Recent penalties include a £130,000 penalty imposed on Powys County Council and £250,000 for the Scottish Borders Council. There have been 19 local authorities "fined" for breaches of security to date.

3.2 The ICO and DCLG recommend some actions that all local authorities can and should take to reduce the likelihood of falling foul of data protection requirements. These include recommendations to:

- Have identified and trained a board-level individual to act as the Senior Information Risk Owner (SIRO);
- Continuously make staff aware of the existing information governance policies and guidelines, emphasising the importance of following them in practice and that a breach of policy will be regarded as a disciplinary matter;
- Ensure all staff undertake regular and relevant information governance training.

It is to be noted that the coverage of "information" extends beyond personal data.

3.3 Currently, the Council's Data Protection Policy places day to day responsibility for compliance with the Act, including data security, with the Managing Directors and Heads of Service within their respective areas of authority under delegated arrangements. Within each Service, a Data Protection Link Officer(s) has/have been appointed by Heads of Service to undertake administration of data protection and to assist in compliance. That role includes ensuring all systems are appropriately notified to the ICO, awareness of the Data Protection Act 1998 (DPA), control of processing of data in compliance with the Councils requirements and assisting in responses to subject access requests.

3.4 These in Service arrangements are aided by the central resource providing general data protection advice. These are coordinated by the Borough Solicitor (part of an overarching role). The central resource includes the Senior Admin & Electoral Services Officer (DP Officer), whose responsibilities include maintenance of the notification of processing with the ICO and the internal register of subject access requests, development of corporate procedures and the first point of contact for subject access requests. Training resources are to be provided from the corporate resource provided through Human Resources (or within a Service, where particular needs are identified). Legal officers provide assistance for the strategic aspects and more complex matters as part of my coordinating role. Formerly the Head of ICT provided the role of developing and enforcing the ICT & data Security Policy, although the change in arrangements through engagement of OCL requires some changes to this allocation of responsibility.

3.5 The policy recognises also that all officers and members have a duty to observe the principles of the DPA when handling personal data.

4.0 ISSUES

4.1 The Council holds a vast amount of data about customers and employees, and its services and properties. This is held both electronically and in paper form. It is vital that proper arrangements are in place to appropriately safeguard this information. The importance of proper information security has been borne out by the number of data losses which continue to be reported across the public sector, showing that threats to our information security are ever-present.

4.2 It is essential to have technical measures in place to mitigate risk, such as encryption of devices (e.g. a programme of encryption of laptops is currently being rolled out); to have policies and procedures to dictate how data/information should

be used and to carry out training and awareness-raising to remind staff to meet requirements. There is also another important element in the information security framework, namely governance. In this context this means that we must have clear responsibilities and reporting lines to ensure that information security is managed properly and that we have a comprehensive view of the state of information security across the Council.

4.3 A Local Government Association (LGA) / Government Connect (GC) document *'Business Case for Creating a SIRO Role'* (Appendix 1) acknowledges that often there is someone already undertaking many of the functions of a SIRO, it recommends that information security is given a higher profile with clear governance arrangements in place to ensure that information security is managed properly. It advises that the key roles in the governance of information security are the SIRO, the Information Security Group (ISG) and the Information Asset Owners (IAOs). All staff, members and partner organisations also have a responsibility to follow security policies.

4.4. SIRO

LGA guidance and best practice recommends that the SIRO:

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

The SIRO is not intended to be a new post but rather a newly defined set of responsibilities for an existing 'board-level' post. It is not concerned solely with ICT, but takes a broader view of our information assets as a whole, in any form. I already undertake a coordinating role and it is therefore proposed that my post should be so designated.

Feedback from other local authorities indicates that the SIRO resides within a Corporate Governance or Legal area of responsibility.

4.5 Information Governance/Data Protection Working Group (the Group)

The LGA guidance recommends that a working group should be set up by the Chief Officer Steering Group or Executive Management Team to look into the state of information security in the Council. This group should be composed of representatives from Legal and Democracy Services, Finance, ICT, Internal Audit, Risk Management and the Data Protection Officer. Representatives of other sections should attend meetings as required. The Group should develop policy and guidance on information security and maintain a reporting procedure for information security breaches. The Group would support the SIRO and its remit would be to:

- Review and develop the Council's information security strategy.
- Review and develop information security policies and guidance and ratify changes to these, including ongoing review of relevant Council Policies, e.g.

Data Protection Policy and ICT and Data Security Policy and Retention and Disposal Policy.
- Coordinate a data protection review within Services, to include: compliance, cataloguing of data resources, training requirements, document assessment, e.g. for privacy notice/customer notification.
- Assist in a coordinated approach to Service Specific Data Protection Procedures
- Assist with management of security risks in projects through the project life cycle
- Review all reported security breaches and report them regularly (and immediately where appropriate) to the SIRO and onward to Government Connect where appropriate
- As appropriate, report information security breaches to the Information Commissioner via the SIRO
- Promote awareness of information security by all officers and Members
- Plan, develop and deliver training on information security in consultation with the Transformation Manager.

It is proposed that the current Data Protection Working Group be renamed the Information Security/Data Protection Working Group with the above terms of reference so as to more closely accord with the LGA guidance. Service Heads and their respective Link Officers would continue to service this group which the SIRO would chair.

4.6 Information Asset Owners (IAO)

LGA guidance and best practice recommends the formal nomination of IAOs. IAOs should be senior managers/software system supervisors across the Council who are currently responsible for the main information systems and information assets.

Relevant senior managers/software personnel have been identified by Heads of Service for formal nomination as IAOs and the role is recognised in the updated Data Protection Policy, attached at appendix 2. In terms of information security their responsibilities would be:

- To manage security, compliance and risks associated with their information assets
- To carry out an annual assessment of information risk as part of risk management
- To ensure that staff accessing the systems are made aware of security issues and acceptable use and receive training as necessary
- To ensure that information security incidents are reported via the Council's information security incident reporting procedure
- To ensure that actions are taken to remedy breaches
- To classify information assets in line with corporate policies. Using a classification scheme for sensitive and confidential information.
- To receive information risk management training annually
- To consider on an annual basis how better use could be made of their information assets within the law

5.0 FINANCIAL AND RESOURCE IMPLICATIONS

5.1 In order to deliver and embed the revised arrangements a one-off £30,000 additional support be sourced to assist Heads of Service in implementing the updated policy and arrangements. This would be used to procure a temporary post enabling the relevant processes etc to be put in place. A bid for the resource would be put forward for consideration at February Council.

6.0 SUSTAINABILITY IMPLICATIONS/COMMUNITY STRATEGY

6.1 Robust information systems have a role in delivering against all of the themes of the community strategy.

7.0 RISK ASSESSMENT

7.1 Good information governance arrangements will establish clear accountability and reporting lines across the Council in relation to data protection and information security. They will assist the Council in securing compliance. The recent internal audit of data management has highlighted certain areas of service delivery which require attention. The consequences of security or other information handling incidents can be significant, particularly relating to personal data loss, in both financial and reputational terms.

Background Documents

There are no background documents (as defined in Section 100D(5) of the Local Government Act 1972) to this Report.

Equality Impact Assessment

The decision does not have any direct impact on members of the public, employees, elected members and/or stakeholders. Therefore no Equality Impact Assessment is required.

Appendices

Appendix 1: The LGA/GC document *'Business Case for Creating a SIRO*
Appendix 2: Updated Data Protection Policy
Appendix 3: Current Data Protection Policy

Business Case for Creating a SIRO Role

Background Information

1. INTRODUCTION

The 2007 HMRC CD incident and subsequent developments have brought the information assurance agenda further up the corporate agenda. The Data Protection act clearly states that organisations MUST look after personal information. The ICO now has the power to impose large fines. Councils hold vast amounts of personal data both electronic and on paper, about customers and employees, and services and properties. Proper arrangements need to be in place to safeguard this information. The importance of proper information assurance and governance, driven by a formal information risk management process, has been borne out by the number of data losses which continue to be reported across the public sector. Recently outbreaks of the Conficker virus in Councils continue to show that threats to information security are ever-present.

It is essential to have technical measures in place, such as encryption, to mitigate the risk, to have policies and procedures to dictate how these should be used and to carry out training and awareness-raising to remind staff to follow these. There is also another important element in the information security framework, namely governance. In this context this means that we must have clear responsibilities and reporting lines to ensure that information security is managed properly and that we have a comprehensive view of the state of information security across authorities.

2. DRIVERS FOR APPOINTING A SENIOR INFORMATION RISK OWNER (SIRO)

Following the loss of data by HMRC and several other security breaches, the Government conducted a review of its data handling procedures and one of its recommendations was that all Government departments should designate a board member as Senior Information Risk Owner (SIRO) and that all information systems should have an Information Asset Owner. The Local Government Association (in its *Data Handling Guidelines*, issued last year) said that all local authorities should do the same. These roles are also well established in the NHS.

As part of their Key Lines of Enquiry (KLOE), many authorities report on their approach to data quality.

In addition to these external drivers, there are other reasons for clarifying roles and responsibilities in relation to information security. As part of the GCSx Code of Connection, it is a requirement to report security incidents to GovCert UK (The CESG Computer Emergency Response Tam), and or a Local WARP Warning,Advice and Reporting Point).

Over the last few years a number of potential and actual security breaches have been reported. Some of these have led to serious consequences and have been reported to the Information Commissioner, who investigates breaches involving personal data. In such cases the Information Commissioner normally checks on the governance arrangements for information security, including whether an organisation has a SIRO. It should be remembered that the Information Commissioner

has the power to compel an organisation to improve its information security arrangements, and some councils have recently had to sign undertakings to this effect. In addition, the Information Commissioner will shortly be given powers to fine organisations that mishandle personal data.

The SIRO role will also support any initiatives to reduce risk following the investigation of security threats such as the Conficker virus.

Councils are currently stepping up awareness-raising for staff on information security and there is a need to identify resources for this. There is often someone already undertaking many of the functions required; this approach simply formalises the ad-hoc arrangements that may be in place. Clarifying the governance arrangements will help to ensure that we get the best value from this investment in the future.

3 INFORMATION SECURITY ROLES

The key roles in the governance of information security are the SIRO, the Information Security Group (ISG) and the Information Asset Owners (IAOs). All staff, members and partner organisations also have a responsibility to follow our security policies.

3.1 SIRO

Local Government Association guidance and best practice elsewhere suggests that the SIRO

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

The SIRO is not intended to be a new post but rather a newly-defined set of responsibilities for an existing 'board-level' post. It is not concerned solely with IT, but takes a broader view of our information assets as a whole, in any form.

Individual authorities will determine exactly where the role and responsibilities lie within the council.

3.2 The Information Security Group (ISG)

A working group set up by the Chief Officer Steering Group or Executive Management Tem to look into the state of information security in the Council. This group is composed of representatives from the Corporate Information Unit, Legal Services, Finance, CICT (Corporate ICT), Internal Audit, Risk Management and the Data Protection Officer. Representatives of other sections attend meetings as required. The ISG has developed policy and guidance on information security and piloted a reporting procedure for information security breaches.

It is proposed that a group should continue to meet and should support the SIRO. Its remit will be to:

- Develop or review an information security strategy for the Council
- Develop information security policies and guidance and ratify changes. New and changed corporate policies are to be approved via the Council's normal process (Example policies can be found on the Government Connect Code of Connection Toolkit site at: www.g3ctoolkit.net
- Assist with management of security risks in projects through the project life cycle
- Review all reported security breaches and report them regularly to the SIRO and onward to GovCert and the WARP.
- As appropriate, report information security breaches to the Information Commissioner via the SIRO
- Promote awareness of information security by all officers and Members
- Plan, develop and deliver training on information security as required

- Produce an annual statement on the security of our information assets for the SIRO, covering breaches, training, results of audits, progress made against the Information Assurance Maturity Model (IAMM), using the Information Assurance Assessment Framework IAAF) etc both available from www.cesg.gov.uk

3.3 Information Asset Owners (IAOs)

IAOs are the senior managers across the Council who are currently responsible for the main information systems and information assets. In terms of information security their responsibilities are:

- To manage security, compliance and risks associated with their information assets
- To carry out an annual assessment of information risk as part of risk management
- To ensure that staff accessing the systems are made aware of security issues and acceptable use and receive training as necessary
- To ensure that information security incidents are reported via the Council's information security incident reporting procedure see www.govcertuk.gov.uk and www.nlawarp.gov.uk
- To ensure that actions are taken to remedy breaches
- To classify information assets in line with corporate policies. Using a classification scheme for sensitive and confidential information.
- To receive information risk management training annually
- To consider on an annual basis how better use could be made of their information assets within the law

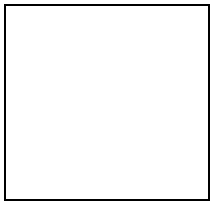
In the main these are not novel proposals but rather the normal responsibilities of senior managers responsible for information systems and assets.

3.4 All staff, Members and partner organisations

All staff, Members and partner organisations that access our information must follow the Council's security policies in handling information in any form. Any deliberate breach of Council policies which compromises the confidentiality, integrity or availability of Council owned information assets may be a criminal offence for which individuals may be personally liable.

For further information contact: mark.brett@lga.gov.uk

We greatfully acknowledge the assistance of the Yorkshire and Humber WARP and Bolton Council in the production of this document.



DATA PROTECTION POLICY

1.0 Introduction

This document sets out West Lancashire Borough Council's policy regarding data protection. The Data Protection Act 1998 and the EC Data Protection Directive form the background to the document. The Policy is drafted using the terms of the Data Protection Act 1998. The Freedom of Information Act affects the Council's use of non-personal information and the operation of this policy. The Human Rights Act 1998 enhances the protection and individual rights give under the Data Protection legislation.

The purpose of the data protection legislation is to regulate the way that personal information about individuals, whether held on computer, in a manual filing system or otherwise, is obtained, stored, used and disclosed. The legislation grants rights to individuals, to see the data stored about them and to require modification of the data if it is wrong and, in certain cases, to compensation. The provisions amount to a right of privacy for the individual.

The 1998 Act requires all processing of personal data to be notified to the Data Protection Commissioner and to be kept and used in accordance with the provisions of the Act.

2.0 Definitions

To aid the understanding of this document and the provisions of the Data Protection Act the following definitions are used:-

2.1 Data is information that is:

- being processed by means of equipment operating automatically in response to instructions given for that purpose e.g. payroll system
- recorded with the intention that it should be processed by means of such equipment (CD ROM)
- recorded as part of a manual filing system or with the intention that it should form part of a relevant filing system.
- one of a number of records to which public access is allowed e.g. information held by the Council (as a Housing Authority) for the purpose of its tenancies.

2.2 Data Controller means the Council as the organisation who determines how data is processed and for what purpose.

2.3 **Data Processor** means any person, other than an employee of the Council, who processes data on behalf of the data controller, e.g. someone contracted to the Council to deal with documents containing personal data.

2.4 **Data subject** is the individual about whom personal data is held.

2.5 **Personal Data** means data about a living individual who can be identified from that information (or from that and other information in the possession of the data controller). This includes an expression of opinion about the individual, and any indication of the intentions of the data controller or any other in respect of that individual.

2.6 **Sensitive Personal Data** means personal data consisting of information as to:-

- racial or ethnic origin of the data subject
- his/her political opinion
- his or her religious beliefs or other beliefs of a similar nature
- whether he or she is a member of a trade union
- his or her physical or mental health or condition
- his or her sexual life
- the commission or alleged commission by him or her of an offence
- any proceedings for any offence committed or alleged to have been committed by him or her, the disposal of such proceedings or the sentence of any court in such proceedings

2.7 **Processing** is very widely drawn and means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including:-

- organisation, adaptation or alteration
- retrieval, consultation or use of,
- dissemination, disclosure or otherwise making available
- combination, blocking, erasure or destruction of the information or data

2.8 **Relevant Filing System** means any information held manually in an organised structure either by reference to individuals or other criteria such that specific information about a particular individual is readily accessible.

2.9 **Special Purposes** means any one or more of the following ie journalistic, artistic or literary.

3.0 Principles

The Data Protection Act 1998 contains 8 governing Principles relating to the collection, use, processing, and disclosure of data, and the rights of data subjects to have access to personal data concerning themselves. These Principles are:-

1. Personal data shall be processed fairly and lawfully and, in particular shall not be processed unless one of the conditions in Schedule 2 of the Act is met. These can be summarised as: where the individual has given consent; where the processing is necessary: for any contract, legal obligation, to protect the vital interests of the individual, or in the interests of justice and in the case of sensitive personal data at least one of the conditions in Schedule 3 of the Act is also met. The Schedule 3 conditions can be summarised as explicit consent, or where necessary for: employment obligations, vital interests, non-profit associations, manifestly made public, legal proceedings, administration of justice, medical purposes, ethnic monitoring

2. Personal data shall be obtained only for one or more specified and lawful purpose and shall not be further processed in any manner incompatible with that purpose or those purposes

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

4. Personal data shall be accurate and, where necessary, kept up to date

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes

6. Personal data shall be processed in accordance with the rights of the data subject under this act (this includes the rights of subjects to access the data and to correct it)

7. Appropriate technical and organisation measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (this relates to data security)

8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

These principles are regarded as the **minimum standards** of practice for any organisation with respect to personal data. Copies of the "Guidelines to the Data Protection Act", which illustrate these 8 principles are available from Sylvia Smith the Snr. Admin & Electoral Services Officer (extension 5031).

4.0 Policy

The Council Supports the objectives of the Data Protection Act 1998. This policy is intended to maintain the confidentiality of personal data held or processed either on computer, in manual files or otherwise and to increase the access given to individuals to information relating to them.

The Policy links to the other Council policies and documents for example:-

- ICT and Data Security Policy
- Retention and Disposal Schedule
- The Council's Constitution

- Code of Conduct
- Human Resources Policies
- Use of Internet & Email
- HIV and Aids Policy

It also links to the information sharing protocol with the Police Authority and to other initiatives under the Crime and Disorder Act 1998. There are a number of procedures underpinning this policy and guidance notes to supplement this policy for example:-

- Subject Access
- Registration/Notification
- New Systems
- Disclosures

To assist officers in complying with their Data Protection duties the Council has produced a collection of guidance notes, each relates to a specific area of data protection/security. These guidance notes are appended to this policy at Appendix 2

4.1 External and Internal Registration/Notification

The Council will have an external notification (registration) with the Information Commissioner which will be supplemented by an **internal register of sources and disclosures.**

4.2 Amount of data to be held

The Council will hold the minimum personal data necessary to enable it to perform its functions. The data will be erased once the need to hold it has passed. Every effort will be made to ensure that data is accurate and up to date, and that inaccuracies are corrected quickly.

4.3 Subject Access

The Council will provide to any individual who requests it, in a specified manner, a reply stating whether or not the Council holds personal data about that individual. A written copy, in clear language, of the current data held, will be given. A fee of £10 will be charged for this service.

4.4 Public Registers

The Council maintains a number of public registers that contain personal data or data that could be used to identify individuals of these are examples set out in Appendix 1. Strict compliance with the legislation giving rights of access will be used in all cases.

4.5 Disclosures

Disclosures of information must be in accordance with the provisions of the Act, the Council's registration/notification and the internal register of sources and disclosures. The Council has a duty to disclose certain data to public authorities

such as the Inland Revenue, Customs and Excise and Benefits agency this will be done in accordance with the statutory and other requirements.

Disclosure within the authority either to Council officers or elected members will be on the basis of a need to know this will be judged when a request for information is made. The minimum of personal data will be made generally available.

4.6 System Design

The Council intends that personal data must be treated as confidential. Computer and other systems will be designed to comply with the Principles of the Data Protection Act so that access to personal data should be restricted to identifiable system users.

4.7 Training

It is the aim of the Council that all appropriate staff will be properly trained, fully informed of their obligations under the Act and aware of their personal liabilities.

4.8 Disciplinary Action

The Council expects all of its staff and members to comply fully with this Policy and the Principles of the Data Protection legislation. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures following from this policy.

5.0 Responsibilities

Overall responsibility for the efficient administration of the Data Protection legislation lies with the **Council** and is exercised by the Cabinet.

5.1 Managing Directors and Heads of Service

Day to day responsibility for administration and compliance with the act is delegated to the Managing Directors and Heads of Service, for compliance with the Act's provisions within their respective areas of authority. Within each Service, Data Protection Link Officers may be appointed to undertake administration of data protection and to assist in compliance with the requirements of the legislation on behalf of the Managing Directors and Heads of Service (the number of Data Protection Link Officers in each Service will be a matter for the Heads of Service to determine).

5.2 Data Protection Officer (Snr. Admin & Electoral Services Officer)

It is the responsibility of the Data Protection Officer to assist the Council to ensure compliance with this policy, to specify the procedures to be adopted and to co-ordinate the activities of the designated Link Officers.

The main duties of the Data Protection Officer are:-

- maintenance of the Council's external registration/notification under the Act, and to act as liaison officer with the Information Commissioner

- development, updating and publication of data protection procedures for the Council.

- maintenance of the internal register of sources and disclosures and in association with the internal Audit Section to audit data protection procedures and practices.

- initial contact point for subject access requests.

- in conjunction with Human Resources, provision of education and training seminars regarding data protection issues

5.3 Senior Information Risk Owner (SIRO)

The Borough Solicitor acts as the Council's SIRO. The SIRO

- is the officer who is ultimately accountable for the assurance of information security at the Council
- champions information security at Directorate Service Head (DSH) level
- owns the corporate information security policy
- provides an annual statement of the security of information assets for the Annual Governance Statement (as part of the audit process)
- receives strategic information risk management training at least once a year

5.4 Information Governance/Data Protection Working Group (the Group)

This group, chaired by the SIRO, is comprised of representatives from Legal and Democracy, Finance, ICT, Internal Audit, Risk Management and the Data Protection Officer. Representatives of other sections attend meetings as required. The Group develops policy and guidance on information security and maintains a reporting procedure for information security breaches. The Group supports the SIRO and its remit is to:

- review and develop the Council's information security strategy.
- review and develop information security policies and guidance and ratify changes to these, including ongoing review of relevant Council Policies, e.g. Data Protection Policy and ICT and Data Security Policy and Retention and Disposal Policy.
- co-ordinate a data protection review within Services, to include: compliance, cataloguing of data resources, training requirements, document assessment, e.g. for privacy notice/customer notification.
- assist in a coordinated approach to Service Specific Data Protection Procedures
- assist with management of security risks in projects through the project life cycle
- review all reported security breaches and report them regularly (and immediately where appropriate) to the SIRO and onward to Government Connect where appropriate

- as appropriate, report information security breaches to the Information Commissioner via the SIRO
- promote awareness of information security by all officers and Members
- plan, develop and deliver training on information security in consultation with the Transformation Manager.

5.5 Information Asset Owners (IAO)

IAOs are senior managers/software system supervisors across the Council who are currently responsible for the main information systems and information assets. In terms of information security their responsibilities are:

- to manage security, compliance and risks associated with their information assets
- to carry out an annual assessment of information risk as part of risk management
- to ensure that staff accessing the systems are made aware of security issues and acceptable use and receive training as necessary
- to ensure that information security incidents are reported via the Council's information security incident reporting procedure
- to ensure that actions are taken to remedy breaches
- to classify information assets in line with corporate policies. Using a classification scheme for sensitive and confidential information.
- to receive information risk management training annually
- to consider on an annual basis how better use could be made of their information assets within the law

5.6 Data Protection Link Officers

The Data Protection Link Officers are responsible to the Managing Directors and Heads of Service for:-

- liaison with the Data Protection Officer on all matters concerning administration of the Act
- working with the Managing Directors and Heads of Service to ensure compliance with the notification (registration) particulars in respect of systems within the Service;
- working with the Service Managers and the SIRO to ensure awareness of the Act within the Service, and to ensure that the control and handling of personal data within the Division does not contravene the Data Protection Principles or Council procedures.
- assisting the Data Protection Officer in the collation and validation of external and internal registration particulars relevant to the Service, and advising the Data Protection Officer of any planned changes to the registration particulars
- assisting in the response to access requests from data subjects.

5.7 Officers and Members

In addition to the formal responsibilities outlined above, all officers and members have a duty to observe the Principles of the Act and the procedures referred to in this document.

Individuals who do not handle personal data as part of their normal work have a responsibility to ensure that any personal data they see or hear goes no further. This includes personal data and information extracted from such data, thus, for example, unauthorised disclosure of data might occur by passing information over the telephone, communicating information contained on a computer print-out or even inadvertently by reading a computer screen.

Disciplinary action may result if the Data Protection Principles or procedures outlined in this document are breached.

(Ref DATA PROTECTION POLICY 17th January 2013)

Appendix 1

Examples of Publicly available information that could be used to identify individuals

Elections
Representation of the Peoples Act 2000
Register of persons who are eligible to vote in elections

Returns or declarations and accompanying documents relating to election expenses sent by a candidate of a parliamentary or local government election to the Council

Disclosable Pecuniary Interests
Local Government Act 2011 - The Relevant Authorities (Disclosable Pecuniary Interests) Regulations 2012.

A register setting out certain information which elected members give on their interests

Members Allowances
The Local Authority (Members' Allowances) Regulations 1991 as amended by The Local Authority (Members' Allowances)(Amendment) Act Regulations 2003

Records of payments made to elected members are open to inspection by local government electors for the area. Additionally, the authority must publish within its own area details of the total sums paid under the scheme.

Committee Minutes Reports etc
Local Government Act 1972

Allows access to agendas and reports of committees and subcommittees. Minutes are also available

Taxis and Private Hire Vehicles
Town Police Clauses Act 1847
Local Government (Miscellaneous Provisions) Act 1976

Register containing information about owners and drivers of taxis and drivers of private hire vehicles.

APPENDIX 2

DATA PROTECTION GUIDANCE NOTES

1. Checking entitlement procedure
2. Email procedure
3. Fax procedure
4. Phone procedure
5. Office security procedure
6. Paper records out of the office procedure
7. Clear desk procedure
8. Checklist for privacy notices on applications and other forms.
9. Procedure for sending personal information in the post
10. Contractor checklist
11. Checklist for data sharing agreement or protocol
12. Building & Network Security Procedure
13. Information Security Incident Management Procedure
14. GCSx Acceptable Usage Policy

WLBC DP GUIDANCE NOTE 1

Checking entitlement procedure

Whenever you receive a request to transfer personal, sensitive or confidential data, the first step to take is to ensure that the person who has asked for the information is who they say they are, and is entitled to receive the information.

Before disclosing any personal, sensitive or confidential information, you should be sure that you know

- Who is asking
- What information they want
- Why they need to know
- Whether they have a legal power to demand the information
- Whether the Council has already agreed to supply the information
- If neither of the above two apply, whether you have the consent of the subject or owner of the information to supply it

With any organisation with whom you have regular, routine contact, you should agree a specific way of asking for information and specific officers who are entitled to ask. This can speed up responses to legitimate requests considerably.

Requests received by phone

- No matter who the caller is, if you are in any doubt about whether the request is valid, ask the caller to put their request in writing

- If the requester is a customer or other member of the public, ask them two questions that only they are likely to know the answer to – a reference number relevant to their service, when their service started, or similar

- If the requester is a family member or friend of a service user or staff member, do not provide information unless you have the person's consent (either previously obtained in writing, or from the person themselves if they are also present on the call). If consent has not been provided, ask for the request to be put in writing, or for the service user to get in touch first

- If the requester is from the police or another official body, ask them to put their request in writing. If they say that the request is an emergency, ask for their name, who they represent, and what data they need and why they need it. If the request is valid, call them back via their switchboard or main contact number, not a direct dial number. Check this on the organisation's website.

Requests received by email

An email address that ends in gov.uk, @police.pnn.uk, @nhs.net, or gscx.gov.uk or gsi.gov.uk is very likely to be valid. An email received from such an address is likely to be genuine, but this does not remove the requirement to check entitlement.

WLBC DP GUIDANCE NOTE 2

Email procedure

1 General advice

All staff, volunteers and contractors need to keep personal information about individuals secure and private at all times. Email is convenient and fast but it carries a series of risks:

- It is very easy to send information to the wrong people
- Data in an email is very portable, and can easily be forwarded to others

Never send an email when annoyed or frustrated. The language and tone of an email should be appropriate for context – an email can have the same legal status as a signed letter on headed paper. Assume that this might happen to your email and write it accordingly. Keep work and personal issues separate. Remember that any personal data may be requested by the person about whom it is recorded.

If sending sensitive or potentially damaging information in an email – stop and think. Is email the best and most secure way to circulate the information?

2 Requirements

- When sending sensitive information (e.g. information about criminal activity, health or other potentially damaging information), use encrypted email where available

- If password-protecting an attached document, do not send the password by email – contact the recipients separately to provide the password, and change it every time. Be aware that dictionary words are not a secure password

- Check that you have used the right email address

- Never let the email software fill in a person's email – type in the whole address, or choose it from an address book. If you have previously emailed a person with a similar name to your recipient, the software might fill in the wrong address

- If copying people into an email, always use the BCC ('blind copy') function unless you are certain that each recipient already knows the other's address. If sending emails to home addresses, use BCC automatically.

- If using an email distribution list, check before sending the email that you have selected the correct one and the only the right people will receive whatever you are sending

- Check that you have added the right attachment before sending an email

- If forwarding information, include only the parts of the email you want the recipient to see. Never forward a long email chain unless you are certain that the recipient is entitled to all of the information in the chain. Look at where the conversation started, and what else is included

WLBC DP GUIDANCE NOTE 3

Fax/Photocopier/Scanner procedure

A. Use of Fax

1. General principles

Fax machines are not a secure method of transmitting information and should only be used if no other method is available. For both confidentiality and legal reasons, it is vital that care is taken when sending a fax. Faxing information carries a number of risks:

- It is easy to fax information to the wrong place by dialling the wrong number or using one which is out of date, and you cannot recall a fax easily
- The quality of copies on arrival cannot be guaranteed - this can lead to inaccuracies and misreading of information
- You do not know who is on the other end of a fax machine, and who might see it when it arrives

2 Procedure for faxing

For staff, volunteers and contractors

When sending a fax containing confidential or personal information, you must always follow this procedure:

- Ask yourself: should I send this as a fax, or is there a safer alternative?

- **Always use a cover sheet** marked 'Private and Confidential' and which contains:

    - A named recipient, or at least a team name

    - Your name, job title, team, location, your telephone number and fax number

    - The number of pages you are sending, including the cover sheet

    - an explanation of what to do if the fax has been received by the wrong person (e.g. contact you immediately, and do not read or share the contents with anyone else)

- Before you send a fax containing personal or other sensitive data, **telephone the intended recipient** to let them know you are sending a confidential fax and agree a fax number.

- Keep any transaction reports or receipts as evidence of where the fax was sent in case it was sent to the wrong person, so you have a chance of contacting the recipient

- **Ask the recipient to ring you back to confirm receipt**, or ring them yourself after you have sent the fax

- Ensure they confirm that all pages have been received

- **If using a pre-programmed fax number, ensure that you choose the right one**, and regularly check that the pre-programmed numbers are still correct

- If you are entering the number manually, **double-check it** to make sure you are using the right number

For Managers

- You must be aware of what your staff are using fax machines for, who they are sending them to, and why fax is being used as an alternative to other methods. Consider whether fax remains the right way to share information – secure email may be an alternative

- Your fax machine should be in a restricted location, not in a public area of your building where faxes can be picked up by anyone who is not part of your team or not authorised to see the information that is being received. If staff pick up your faxes from a central location, they must be instructed not to read faxes, and to bring them straight to your team. You should consider whether this arrangement is secure.

- You should ensure that a member of your team regularly checks any pre-programmed fax numbers to ensure that they remain correct and up-to-date

B. Photocopying, Printing and Scanning

You must ensure that you take all copies of information from the machine once you have finished copying and do not leave any personal information at the copier.

If you send information to a printer used by other members of staff you must always collect your printing straight away and not leave it on the printer allowing other people to see/take the information.

If you are scanning any information, you must ensure that you send it to the correct recipient. As with email, if you are using a recipient distribution list then you must check before you send the scanned information that you have selected the correct recipient and that only the right people will receive whatever you are sending.

WLBC DP GUIDANCE NOTE 4

Phone procedure

1 General principles

For both confidentiality and legal reasons, it is vital that care is taken when providing or receiving information over the phone. Sharing information over the phone carries a number of risks:

- Information may be transcribed incorrectly
- You cannot always be certain who you are speaking to
- You can be overheard

2 When a member of the public calls you

- Ask at least two security questions, appropriate to the service you work in for example a reference number for the service and when their service started. Tell the caller you are asking these questions to make sure that you are dealing with the right person – **do not mention Data Protection.**
- If they are asking about someone else's case or problem, do not provide personal information unless you have the person's consent (either previously obtained in writing or from the person themselves if they are also present on the call). If consent has not been provided, politely explain that you need consent to continue, ask for the request to be put in writing or for the service user to get in touch first to authorise you speak to a nominated person on their behalf.

3 When someone from another organisation calls you asking for information

- Identify the person clearly, check who they work for and what they want
- If they demand information, check their entitlement to demand it – ask what law or right allows them to demand the information
- Unless you are certain that the person is who they say they are, get their switchboard number (not their direct number) and ring them back. Check the switchboard number from their website, not from them
- If in doubt, ask them to put the request in writing

4 When you call someone

- If calling to provide information, be certain that the phone is the best way to provide information – would a fax or email be better (both allow a specific record of the information to be provided)?

- Ensure you speak to the person who needs the information – do not leave personal or sensitive data in a message

5 When someone calls to provide you with information

- Ensure you record information accurately – check the information with the person providing it. Do you have the spelling, numbers and details right?

Remember: Security questions are only necessary when you are being asked to disclose personal information.

WLBC DP GUIDANCE NOTE 5

Office security procedure

1 Introduction

Trustworthy and trusted staff are the best defence against internal and external security threats, but they must be supported by sensible procedures.

Managers must take all reasonable steps to ensure that information is secure. You should remember that you are protecting personal information as much from accidental disclosure as deliberate theft**.**

Managers must ensure the following:

- The workplace is secure, and the risks have been properly assessed
- All staff have received Data Protection and confidentiality training
- All staff have read and understood policies on Data Protection, information security, appropriate IT usage, and information sharing

2 General office checklist

- Are paper files containing personal data locked away when not in use?
- In areas accessible to the public, have you ensured that there is no personal data on display (i.e. on whiteboards or noticeboards)?
- In open-plan offices, are there secure areas for confidential discussions and phone calls?
- Are offices where personal data is stored or on display used as thoroughfares to other parts of the building? If so, are measures in place to protect the data from being seen?
- Are computer screens not visible in areas to which the public have access, and are they angled away from windows?
- Do you ensure that passwords or login information are not written down, or recorded anywhere? Do not allow anyone else to use your password.
- Change your password regularly and immediately if you think someone else has identified it.
- Are PCs and laptops set up to log out when not in use?
- Do managers authorise the removal of paper files from the office?
- Is there a system in place to log the removal of paper files from where they are stored (either a file removal form left in where they are stored, or an electronic record)? This should show who has a file, and if it is removed from the office, where it is being taken to.
- Confidential files should be password protected if there is a risk of them being accessed by unauthorised staff.
- Is there an effective back up system in place and is data stored on a shared sever file where possible?

- Passwords should only be used by the authorised owner. Enhanced password controls on the Authority's network include the following restrictions:
- Minimum of 7 characters
- Must not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Must contain characters from three of the following categories:
    1. English uppercase characters (A through Z)
    2. English lowercase characters (a through z)
    3. Base 10 digits (0 through 9)
    4. Non-alphabetic characters (e.g. !, $, £, %)
- Must be changed a minimum of every 90 days
- Must not be used within 20 password changes

- Forgotten passwords can only be reset by contacting the ICT Service Desk on 0845 053 0042 or email: ICT Servicedesk@oneconnectlimited.co.uk

3 Visitors

Office areas should be open and welcoming, but security measures must be in place. Offices that do not have access controls need different forms of security to places where access is controlled.

- All areas where sensitive information is used or stored should introduce access controls where they are not already in place
- Contractors should sign, or have in place, a confidentiality agreement when entering the premises.
- All visitors should be obliged to sign-in, wear an ID badge and should generally be accompanied when on site.
- If a contractor or visitor requires either a door access swipe and/or network login submit their details to Admin & Elections and ensure that the door access swipe is retrieved before the contract/visitor leaves the site and, if they have been provided with a network login, that the ICT Service Desk is informed to ensure network access is disabled.

- Anyone not displaying an ID badge should be challenged, asked who they are and where they are going

4 End of the day

- Paperwork should be cleared from desk
- All filing cabinets and drawers should be locked
- Portable electronic equipment – laptops, memory sticks, mobile phones – should be out of sight and locked away
- All windows should be closed and locked
- Curtains and blinds should be drawn to deter opportunist thieves

5 Physical disposal of information

If information is not shredded within the office, confidential waste bins must be available. These should be sealed – confidential waste bags should only be used as a short-term measure. Bags of confidential waste must never be left out for any period of time. All shredding must be undertaken in accordance with the Council's Retention and Disposal Schedule and a record of files destroyed must be maintained.

6. Staff leaving the Council

When staff leave the employment of the authority, it is the responsibility of their line manager to notify the ICT Services to enable their network logon to be disabled and to remove the ID and password from the system that the member of staff used. In addition, Admin and Elections should be informed so that the door access is disabled.

7. File review

All files (including physical and electronic files and/or records) should be reviewed periodically. Reviews should take place at least once a year and, more frequently if circumstances require, to ensure the obligations set out are followed. Current working files should be continually monitored and therefore should always be compliant with the requirements of the Act. All officers are responsible for ensuring that their files comply. Closed files should be reviewed in accordance with a programme for review agreed with the Link Officer (most probably dictated by the type of personal data held and the subject area of the file).

Manager see also the Building Security Procedure

WLBC DP GUIDANCE NOTE (6)

Records out of the office procedure

1 Introduction

Staff who need to use paper records containing personal or other confidential data out of the office should ensure that the records must be safe at all times. An encrypted laptop or other form of remote, secure access to information may be a safer alternative and should always be considered. Managers should be aware that their staff are removing files from the office, and ensure that this procedure is followed.

2 Basic principles

- Managers should approve the circumstances in which paper records are removed from the office, and by whom

- The removal of a file from the office should be logged – the log must identify where the record has been taken, when, why and by whom.

- Records should be removed only where necessary, and only for the minimum time required. They should be returned as soon as possible.

3 Records out of the office

- Staff carrying paper documents are responsible for their safety – even if they are carrying documents for someone else.

- Files or folders should only be removed if in a safe and transportable state. There must be no loose papers. A file that is damaged or too large should be re-filed and restored before being taken out

- Files or documents should always be carried in a bag when out of the office. Paper records should not be carried loose. Even if documents are held in a robust file, that file should be carried in a lockable, waterproof bag. An open shopping or carrier bag is never an appropriate way to carry personal data, or confidential or sensitive documents

- Where records are routinely removed from the office as part of the normal course of work, a lockable case or bag should be available at the office

- Where larger quantities of records are routinely removed from the office, a lockable wheeled case should be available at the office

- Under no circumstances should staff read files or records containing personal data on public transport, in restaurants or cafes, or anywhere else where they can be overlooked

- Never leave documents, files or folders unattended, or on show in a car or other vehicle. Always lock them in the boot.

- Before leaving any building, car or public transport, and before you drive away from any location where you have been using paper records, staff should make a conscious check that they have everything with them.

- Paper records should only be in transit during the working day – staff must not carry paper records to pubs, restaurants or other social venues

4. Records at home

- Never leave paper records in your car overnight. If you need to return home with documents containing personal or sensitive data, take them into your home and keep them safe. Ensure that family members do not read or access them.

- If you leave records at home for any reason when you are not there, they should be stored out of sight in a cupboard or drawer.

- Do not store paper records with laptops or other valuables.

5. Use of Portable Computers, PDAs and Mobile Phones for Remote and Homeworking

- Mobile devices, hard copy documents and files should only be removed from the office when that removal has been appropriately authorised. When laptop computers are being transported a carrying case should preferably be used to reduce the risk of accidental damage.

- Computer equipment must not be left unattended in a vehicle unless all doors, windows and other means of access have been secured and locked and all keys of the vehicle removed to a place of safety, and the equipment placed in the boot of the vehicle. The insurers accept that the rear compartment of a hatchback vehicle is considered to be the boot as long as the equipment is stored under the factory fitted cover. Failure to adhere to this will mean that insurance cover will not be available. In the case of overnight storage this should be in a secure building e.g. an officer's house.

- Laptops, memory sticks and removable disks should be encrypted and/or password protected when taken out of the office. Mobile phones and other palm top devices e.g. PDAs should also be password protected. For guidance contact the ICT Service Desk on 0845 053 0042 or email: ICTServicedesk@oneconnectlimited.co.uk.

- All reasonable precautions must be taken to prevent or minimise accident, injury, loss or damage.

- The users of portable computers in a public place should be vigilant as theft is common. Sensitive information should not be displayed in a public place where it could be overlooked.

- No sensitive information should be held on the computer hard drive. Sensitive information should not be transported outside the United Kingdom.

- Only those with legitimate or approved access must use the computer equipment.

- Only software authorised by the Authority must be used. Security backups of data should be taken on a regular basis.

- If any computer equipment, PDA or mobile phone is lost or stolen then this should be reported to the ICT Service Desk on 0845 053 0042 or email: ICT Servicedesk@oneconnectlimited.co.uk.

WLBC DP GUIDANCE NOTE (7)

Clear Desk Procedure

1 General principles

The purpose of a clear desk procedure is to limit the risk of paper records being lost, stolen, inappropriately accessed or damaged by contractors and visitors, staff not directly involved in providing services to the individual, or even thieves and vandals. The principle for handling records should be as follows: **information of any kind should be accessible only to those who need it, and only when they are using it.**

2 Practical measures

2.1 Paper records

- Desks must be cleared of any confidential or person identifiable information when you leave the office for the day

- Where available, paper should be stored in locked cabinets or other secure furniture when not in use. Where secure storage is not available but is deemed appropriate, this should be raised with managers.

- Where lockable furniture is not available, the doors to the office must be locked by the last person to leave

- Confidential or personal information, when printed, should be removed from printers or faxes immediately

- Paper records which are no longer required must be stored securely for disposal, which should happen as soon as possible

- In a public area, or an area to which the public or visitors have routine access, no paper files or records should be left out unless the visitor is supervised at all times

- Keys used to lock away records should not be left on display, and should be locked in a key cabinet where available. The codes for doors or locks must never be on display.

- Visitor, appointment or message books should be locked away when not in use.

2.2 Computer records

- Passwords must not be written down and you should not tell anyone (or allow someone else to use) your password. Users should change their passwords regularly and immediately if they believe someone else has

identified it. Personal data must only be held on a PC which is password protected and/or encrypted to prevent authorised access.

- Screens must be locked when computers are left unattended, irrespective of the amount of time spent away

- Screen locks should be used, so that a computer locks itself if left unattended

- Computer screens should be positioned away from the view of visitors or the public, and angled away from windows

- Where it is not possible to position screens out of sight, they should be closed, minimised or locked when unauthorised persons are in close proximity

Consideration should be given to the use of staff's personal mobile phones/cameras in the office and whether this is a security concern

WLBC DP GUIDANCE NOTE (8)

Checklist for privacy notices on application and other forms

The purpose of a privacy notice is straightforward: it tells the person whose information is being gathered what you intend to do with their information and who you will share it with or disclose it to. There is a fundamental difference between telling someone how you are going to use their personal information and getting their consent for it so it is important to be certain about which one you are doing.

The collection and use of personal information is often essential to provide the service the individual has requested and/or may be required by law and therefore choice is not an issue.

If you are telling the person what happens to their data, this is a privacy notice. The privacy notice should be a clear description of what you are going to do, using a simple to understand heading i.e. 'How we use your information".

If you are asking the person for permission to use their data, then the privacy notice should come first, and then you should ask for consent in a clear and unambiguous way. Bear in mind that if you are asking for consent, if the person refuses, you should respect that. You can, nevertheless, point out what will happen if they do refuse.

If the use of data is complicated, give the person the main points on your form, and then tell them where they can find more detail (for example you can have a layered privacy notice with the main headlines on an application form, and then a website page or a separate leaflet).

- Before you start, has the amount of information being requested been measured against the purpose for which it is being gathered? Is anything being asked for that is not really needed, and is there any data that is required that is not asked for on the form?

- Is the form in plain English, making clear what the person is being asked for, and why the information is being gathered?

- Could any of the information gathered be taken anonymously, and still achieve the same objective?

- Have you provided enough options to allow people to give full and accurate answers?

- Is any check or verification carried out on the information (i.e. taking up references, credit check)? If so, is this made clear?

- Is any of the information collected shared with another organisation like the council, voluntary organisation or health bodies? If so, have you made this clear and told them who you will share it with?

- Is the information that you are collecting used for any purpose not stated on the form? For example, is feedback or complaints data being used to make decisions about services provided to a resident? If so, this must be explained clearly on the form or as part of the process.

- Is the person whose data is being collected likely to be surprised by how their data is being used? If so, what can you do to prevent that?

- Are the replies to questions mandatory or voluntary?

- Does the notice explain the consequences of not providing the information? For example non receipt of a benefit

- Does it explain what you are doing to ensure the security of their personal information?

- Does it explain their rights and how they can exercise them? For example the fact that they can obtain a copy of their personal information or object to direct marketing

- Does it explain who to contact if they want to complain or know more about how their information is being used?

- **Remember to review your privacy notices regularly**

Examples of clauses to be used in a privacy notice: These would need to be tailored to each service:

How information about you will be used.

We collect personal information when you register with us to request a service, when you voluntarily complete customer surveys and provide feedback.

We collect information about you to provide you with a required service and to manage your account.

We may share your information with credit reference agencies and other companies for use in credit decisions, for fraud prevention and to pursue debtors.

We would like to send you information about our own products and services, as well as those of selected third parties, by post, telephone, email and SMS. If you agree to being contacted in this way, please tick the relevant boxes.

□ Post □ Phone □ Email □ SMS

We would also like to share your information with other companies so that they may send you information about their products and services, by post, telephone, email and SMS. If you agree to your information being shared in this way, please tick the box □

You have the right to request a copy of the information that we hold about you. If you need any further information on how your information is being used, if you require a copy of the information we hold or if you wish to make a complaint then please contact……

WLBC DP GUIDANCE NOTE (9)

Procedure for sending personal information in the post

1 Introduction

When sending out paper documents containing personal data, you must ensure that documents are secure and properly addressed. You should bear in mind that some methods of post are more secure than others. The more sensitive the information being sent, the more secure the method of transmission required.

The person sending the document is responsible for ensuring that they are sent to the right people, safely packaged, and that they can safely be returned if not successfully delivered.

Some of the risks involved in posting out records include:

- Using a previously written letter or document as a template but leaving addresses or other inaccurate data in the new document
- Sending the wrong documents out, or using the wrong address

2 For staff, volunteers and contractors

YOU MUST:

- Send only documents that are required rather than whole files. Consider whether a copy of the document, rather than the original would suffice. The loss of a copy is a less serious incident than the loss of the original.

- Ensure that the destination you are sending documents to is still in the same place – especially if the recipient is outside the Council.

- Check the address to ensure that it is correct, and send documents to a named person if at all possible, and not to a department or team.

- Check **everything** that you put into the envelope or package, no matter how much of a hurry you are in. Ensure that only the documents you intend to send are included.

- Always put either a covering letter or a compliment slip containing your contact details in the envelope with the information – DO NOT put records or data into an envelope by themselves

- Write your return address on the back of the envelope or package – this will allow a wrongly delivered envelope to be returned without having to be opened

- Seal the envelope securely and mark it Private and Confidential

- Send any personal or other sensitive information by recorded delivery, and keep the tracking information so you can find out when it was delivered

WLBC DP GUIDANCE NOTE (10)

Contractor checklist

A data processor may be a courier who you regularly use to transfer your records, an IT specialist coming in to work on your systems, a consultant or a contractor to whom you outsource work, projects or services. If they handle, analyse, cleanse, send out, shred or collect data for your purposes, you should ask these questions BEFORE you complete a contract. No matter how good a job your contractor does, if you do not get security protections in writing, you do not have them. They are not liable for security breaches – you are.

1 Have you got a written agreement or contract with your processor, which sets out what the job is, and how any personal data will be used?

2 Does it include guarantees that the contractor has adequate security in place to look after your data and require the contractor to act only on your instructions?

3 In general, are the security arrangements set out in the contract at least as strong as the security you have in place when using the data you intend to supply to them?

4 Have you specifically set out what security arrangements they should put in place? This will depend on the arrangement, but some examples include:

- Have you insisted that any laptops, pen drives or other portable media are encrypted?
- Have you required the contractor to put in place appropriate security when moving paper records around?
- Have you insisted on secure storage when personal data is held at their premises – does paperwork need to be locked away, is information stored on systems which have anti-virus protection, back-ups and firewalls

5 Have you set out what will happen to data when the project is completed – i.e. destroy data with confirmation or return all copies to you?

6 Have you set out restrictions on what the contractor can do with the data, whom they can share it with, and which of their staff is entitled to access and use the data? Make sure the organisation has appropriate security checks on their staff.

7 Have you confirmed that the contractor cannot use the data for their own purposes, and cannot disclose it to a third party without your express permission?

8 Have you put in place a mechanism to monitor the contractor's compliance with these arrangements?

9. Make sure the contract requires the contractor to report any security breaches or other problems to you and have procedures in place on how you will act if a problem is reported.

Below are some examples of a DPA clause for inclusion in contracts. These are examples only and in every case when you are engaging a contractor you will need to ensure that suitable clauses are in place to protect the Council. Please consult your manager and Legal Services if in any doubt.

The Council is the data controller for the purposes of the Data Protection Act 1998 and the Contractor hereby undertakes that any personal data provided under this Agreement shall be dealt with by him only in accordance with the instructions of the Council and at all times within the requirements of the Data Protection Act 1998 (as amended from time to time). Without prejudice to the generality of the foregoing the Contractor shall:

- have and maintain in place technical and organisational measures governing the processing of the Council's personal data in accordance with the requirements of the seventh data protection principle;
- take all reasonable steps to ensure the reliability of any employees who may have access to the Council's personal data;
- prevent disclosure of any personal data supplied by the Council other than to those members of staff who necessarily require that data for the purposes of carrying out the Contractors obligations under this Agreement.

The Contractor hereby agrees to supply to the Council upon request and within 10 days all information supplied or obtained in the carrying out the agreement as required from the Council in accordance with a request made to it under the Freedom of Information Act 2000.

Or

Data Protection

(a) Without prejudice to any other obligations herein the Contractor shall:

(i) comply with each of the provisions of the Data Protection Act 1998 ("the Act") as amended or replaced from time to time, together with any regulations or Codes of Practice for the time being in force in relation to the Contract Works as if it were a data controller including without limitation the data protection principles set out in Schedule 1 to the Act;

(ii) carry out all data processing in compliance with the requirements of the Act and all equivalent legislation in any other country. In particular, it will comply at all times with good industry practice which shall mean that it shall exercise the degree of skill, due diligence, prudence and foresight that would reasonably and ordinarily be expected from a skilled and experienced person engaged in the provision of personal data processing services;

(iii) only process personal data that it will be processing on the Council's behalf as instructed by the Council. The Contractor shall not carry out any other processing use or disclosure using such personal data.

(b) Security Measures – The Contractor shall:

(i) have in place and at all times maintain appropriate technical and organisational security measures governing the processing of the Council's personal data in accordance with the requirements of Schedule 1, Section 7 of the Act.

(ii) meet to discuss the processing the state of technological development and the best methods by which personal data may be kept secure, up-to-date, and assessed for relevance, accuracy and adequacy, and to plan for the implementation of any new security procedures relating to the processing of personal data.

(c) Employees – The Contractor:

(i) undertakes to take all reasonable steps to ensure the reliability and suitability of any employees who may have access to the Council's personal data.

(d) General – The Contractor shall:

(i) notify the Council immediately of any notice of non-compliance with or request for information under the Act (or any equivalent legislation in any other country) and co-operate fully and promptly and to provide to the Council all reasonable assistance in dealing with any such notice or request;

(ii) not under any circumstances transfer any of the personal data that it may process on the Council's behalf to any country or territory outside the European Economic Area without the Council's prior written consent which may be withheld in its absolute discretion;

(iii) on termination of this agreement for any reason, immediately cease all processing of the Council's personal data and will return to the Council in a format specified by the Council or destroy as the Council may request in its discretion all personal data processed by the Contractor on the Council's behalf

WLBC DP GUIDANCE NOTE (11)
Checklist for a data sharing agreement or protocol

Each question comes from the Information Commissioner's Code of Practice on Data Sharing – the answer to each question should be yes.

	Element of Code of Practice	Yes
1	Is the objective for sharing data set out in the protocol?	
2	Is the legal justification for sharing set out in the protocol?	
3	Are organisations signing up to the protocol included in the document?	
4	Is the data that needs to be shared required described in detail?	
5	Is the way data should be shared included, including nominated people or roles who need to send / receive data?	
6	When and how often will data be shared?	
7	Is there a mechanism for checking the effectiveness of the protocol?	
8	Have the risks of sharing been documented?	
9	Are security measures documented in the protocol	
10	Has the necessity of sharing been assessed?	
11	Have protocol signatories checked / amended their notifications?	
12	Will any data be transferred outside EEA and are processes related to this documented?	
13	Are DPA Principle 1 conditions properly addressed?	
14	Is DPA Principle 1 fairness properly addressed?	
15	Does the protocol include provision for data quality to be confirmed before sharing? • Accuracy • Agreed format for sharing data • Compatibility of systems • Retention / deletion of data • Correction of inaccurate data	
16	Does the protocol include procedures for subject access requests, complaints and queries from data subjects?	
17	Does the protocol include requirements for staff training?	
18	Does the protocol include sanctions for corporate failure to comply with the protocol?	
19	Does the protocol include procedures for dealing with breaches of security and other breaches of the Data Protection Act, duties of confidentiality and other legal obligations?	
20	Are breaches clearly defined?	
21	Does the protocol include a process to terminate the agreement?	
22	Does the protocol set out processes for reviewing the basic necessity of data sharing?	

WLBC DP GUIDANCE NOTE (12)

Building and Network Security Procedures

To ensure the security of corporate buildings and the authority's corporate network please can all managers adhere to the following procedure for door access swipe cards and/or network usernames for new starters, contractors, visitors and other third parties.

1. New Member of Staff (including Agency Staff)

When a new member of staff starts, it is the responsibility of the line manager to provide the Admin and Elections section with the following information.

- Name of new employee
- Section/Service
- Photograph (This can be e-mailed if you have access to a camera, otherwise please bring the member of staff to the Admin and Elections office to have their photo taken)
- Payroll Number
- Car Registration (if applicable)
- Whether the cards should be sent via internal mail or collected.

If access to the Council network is required, please e-mail the ICT Service Desk the following details:

- Name of new employee
- Section/Service
- Job Title
- Which systems the user will require access.

The login details will then be e-mailed back to you. When the user logs in for the first time they will then be asked to create a new unique password.

2. Staff Leaving

When a member of staff leaves it is the responsibility of the line manager to inform the Admin and Elections Section and the ICT Service Desk to ensure that their door access permission and ICT network username are deleted/disabled. Systems Administrators should be instructed by the line manager to remove the ID and password from the application software system that the member of staff used.

Please ensure that their door access swipe card is retrieved on the last day of employment.

3. Contractors/Temporary Passes

Any visitors accessing the back offices at 52 Derby Street must obtain a visitor badge from reception and wear this whilst on the premises. Officers organising meetings in the Council Chamber/Cabinet-committee room do not need a visitors badge but the officer organising the meeting will be responsible for their visitor(s) at all times. You must ensure that your visitor(s) returns their visitors badge at the end of the visit.

If a contractor or visitor requires either a door access swipe and/or a network logon, the line manager should provide Admin and Elections and/or the ICT Service Desk with the following relevant details:

- Name
- Company
- WLBC member of staff they are working for/visiting.
- Which system(s) they require access to.
- How long they plan to be onsite.

The line manager should ensure that the door access swipe card is retrieved before the contractor/visitor leaves the site and if they have been provided with a network logon that the ICT Service Desk is informed to ensure network access is disabled.

In addition to the above procedure and to further enhance building and network security, any swipe card or network login not used within a 2-month period will be disabled.

If you have any queries regarding this procedure, please contact either ICT Service Desk on 0845 053 0042 or email: ICT Servicedesk@oneconnectlimited.co.uk or Admin and Elections (EXT 5013).

WLBC DP Guidance note 13

Information Security Incident Management Procedure

If despite the security measures you take to protect the personal data you hold a security breach occurs, it is important that you deal with the breach appropriately.

Scope

This procedure applies to all Employees, Councillors, Agency Staff, Partners, and contractual third parties of the Council who use or have access to, or custody of WLBC personal data.

All users must understand and adopt this procedure and are responsible for ensuring the safety and security of the Council's personal data that they use or have access to.

A data security incident can happen for a number of reasons ie loss or theft of data or equipment on which data is stored, inappropriate access controls allowing unauthorised use, equipment failure, human error, hacking attack, blagging offences where information is obtained by deceiving organizations who holds it.

Management of Information Security Incidents and Improvements

A consistent approach to dealing with all data security events must be maintained across the Council. Such events must be analysed, and the SIRO must be consulted, for the Head of Service/Managing Director to establish when a security event should be escalated to an information security incident. The incident response procedure must be a seamless continuation of the event reporting process and must include contingency plans to advise the Council on continuing operation during the incident.

Collection of Evidence

If an incident requires information to be collected for an investigation, strict rules need to be adhered to. On no account should managers attempt to investigate incidents themselves. They should refer them to the appropriate officers in accordance with the Councils Data Protection Policy and Anti Fraud and Corruption Strategy and Disciplinary Procedures etc.

Responsibilities and Procedures

Management responsibilities and appropriate procedures are established to ensure an effective response against security events. When an incident is discovered the Head of Service/Managing Director must be informed immediately. The SIRO must advise the Head of Service/Managing Director so they may determine the most appropriate response.

An incident management record must be created and include details of:

- Identification of the incident, analysis to ascertain its cause and vulnerabilities it exploited.
- Limiting or restricting further impact of the incident.
- Tactics for containing the incident.
- Corrective action to repair and prevent reoccurrence.
- Communication across the Council to those affected.

The actions required to recover from the security incident must be under the control of the Head of Service/Managing Director. Only identified and authorised staff should have access to the affected systems during the incident and all of the remedial actions should be documented in as much detail as possible

Learning from Information Security Incidents

To learn from incidents and improve the response process, a Post Incident Review must be conducted. The following details must be retained:

- Types of incidents.
- Volumes of incidents and malfunctions.
- Costs incurred during the incidents.

The information must be collated and reviewed on a regular basis by ICT and any patterns or trends identified. Any changes to the process made as a result of the Post Incident Review must be formally noted.

Information Commissioner's Office

Although there is no legal obligation in the DPA for data controllers to report breaches of security which result in loss, release or corruption of personal data, the IC believes that serious breaches should be brought to the attention of his Office. The nature of the breach or loss can then be considered together with whether the data controller is properly meeting his responsibilities under the DPA.

"Serious breaches" are not defined. However, in considering whether breaches should be reported you need to take into account the potential harm to data subjects, the volume of personal data lost and the sensitivity of the data.

There is a presumption that the matter should be reported where a large volume of personal data is concerned and there is a real risk to individuals suffering some harm.

However, it may be appropriate to report much lower volumes in some circumstances where the risk is particularly high due to the circumstances of the loss or the extent of information about an individual.

The Head of Service/Managing Director shall, in consultation with the SIRO, shall determine whether to report the data security incident to the ICO.

Serious breaches should be notified to the ICO by email using the address casework@ico.gsi.gov.uk or by post to Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Further guidance on how to manage a data security breach can be found on the Information Commissioners website:

http://www.ico.gov.uk/for_organisations/data_protection/the_guide/~/media/documents/library/Data_Protection/Practical_application/guidance_on_data_security_breach_management.ashx

WLBC DP GUIDANCE NOTE 14

Government Connect

Government Connect is a national program which is intended to provide a way for authorities to exchange information with each other, central government, the police, NHS etc in a secure, authenticated way.

The Council is linked to the Government Connect GCSx network for the transferring of sensitive or restricted information between the authority and other local authorities and government departments. To ensure compliance, the Council must comply with the requirements of Government Connect.

Officers who handle sensitive or restricted information as categorised by Government Connect must be made aware by their line manager of the impact of the loss of such material and the actions to take in the event of such a loss. The criteria for assessing sensitive information includes anything that may:

- Cause substantial distress to individuals
- Cause financial loss or to facilitate improper gain or advantage for individuals or companies
- Prejudice the investigation or facilitate the commission of crime
- Breach undertakings to maintain the confidence of information provided by third parties
- Undermine the proper management of public sector and its operation.

A more detailed explanation of these criteria can be found at: www.cabinetoffice.gov.uk/spf/sp2_pmac.aspx

Each user of the network connected to GCSx who has regular access to sensitive information or information that originates from the Government Secure Intranet (GSI) MUST be at least cleared to the Baseline Personal Security Standard (BS). Whilst BS is not formal security clearance, BS provides a level of assurance to the trustworthiness and integrity and probable reliability of prospective employees. A BS check involves verification of: identity, last 3 years employment history, nationality and immigration status and criminal record (unspent convictions only). Contact the HR team for further information

If an officer requires access to the GCSx network, then they must sign the GCSx Acceptable Use policy below:

WLBC GCSx Acceptable Usage Policy

I understand and agree to comply with the security rules of West Lancashire Borough Council as well as the GSi CoCo.

For the avoidance of doubt, the security rules relating to secure e-mail and ICT systems usage include:

I acknowledge that my use of the GSi may be monitored and/or recorded for lawful purposes;

I agree to be responsible for any use by me of the GSi using my unique user credentials (user ID and password, access token or other mechanism as provided) and e-mail address; and

will not use a colleague's credentials to access the GSi and will equally ensure that my credentials are not shared and are protected against misuse;

and will protect such credentials at least to the same level of secrecy as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at my employer's premises); and

will not attempt to access any computer system that I have not been given explicit permission to access;

and will not attempt to access the GSi other than from IT systems and locations which I have been explicitly authorised to use for this purpose; and

will not transmit information via the GSi that I know, suspect or have been advised is of a higher level of sensitivity than my GSi domain is designed to carry; and

will not transmit information via the GSi that I know or suspect to be unacceptable within the context and purpose for which it is being communicated; and

will not make false claims or denials relating to my use of the GSi (e.g. falsely denying that an e-mail had been sent or received); and

will protect any sensitive or not protectively marked material sent, received, stored or processed by me via the GSi to the same level as I would paper copies of similar material; and

will not send Protectively Marked information over public networks such as the Internet; and

will always check that the recipients of e-mail messages are correct so that potentially sensitive or protectively marked information is not accidentally released into the public domain; and

will not auto-forward email from my GSi account to any other non-GSi email account; and

will disclose information received via the GSi only on a 'need to know' basis; and

will not forward or disclose any sensitive or protectively marked material received via the GSi unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel; and

will seek to prevent inadvertent disclosure of sensitive or protectively marked information by avoiding being overlooked when working, by taking care when printing information received via the GSi (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc.) and by carefully checking the distribution list for any material to be transmitted; and

will securely store or destroy any printed material; and

will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via the GSi (this might be by closing the e-mail program, logging-off from the computer, activate a password-protected screensaver, etc., so as to require a user logon for activation); and

where my organisation has implemented other measures to protect unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked or to display a screensaver or similar, requiring a user logon for reactivation), then I will not attempt to disable such protection; and
will make myself familiar with the security policies, procedures and any special instructions that relate to the GSi; and

will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security; and

will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended; and

will not remove equipment or information from my employer's premises without appropriate approval; and

will take precautions to protect all computer media and portable computers when carrying them outside my organisation's premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist thief); and

will not introduce viruses, Trojan horses or other malware into the system or GSi; and
will not disable anti-virus protection provided at my computer; and

will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that my employer informs me are relevant; and

if I am about to leave my employer, I will inform my manager prior to departure of any important information held in my account.

Signed: _____ Date: _____

tsdataprotectionpolicy

DATA PROTECTION POLICY

1.0 Introduction

This document sets out West Lancashire Borough Council's policy regarding data protection. The Data Protection Act 1998 and the EC Data Protection Directive form the background to the document. The Policy is drafted using the terms of the Data Protection Act 1998. The Freedom of Information Act affects the Council's use of non-personal information and the operation of this policy. The Human Rights Act 1998 enhances the protection and individual rights give under the Data Protection legislation.

The purpose of the data protection legislation is to regulate the way that personal information about individuals, whether held on computer, in a manual filing system or otherwise, is obtained, stored, used and disclosed. The legislation grants rights to individuals, to see the data stored about them and to require modification of the data if it is wrong and, in certain cases, to compensation. The provisions amount to a right of privacy for the individual.

The 1998 Act requires all processing of personal data to be notified to the Data Protection Commissioner and to be kept and used in accordance with the provisions of the Act.

2.0 Definitions

To aid the understanding of this document and the provisions of the Data Protection Act the following definitions are used:-

2.1 **Data** is information that is:

- being processed by means of equipment operating automatically in response to instructions given for that purpose e.g. payroll system
- recorded with the intention that it should be processed by means of such equipment (CD ROM)
- recorded as part of a manual filing system or with the intention that it should form part of a relevant filing system.
- one of a number of records to which public access is allowed e.g. information held by the Council (as a Housing Authority) for the purpose of its tenancies.
-

2.2 **Data Controller** means the Council as the organisation who determines how data is processed and for what purpose.

2.3 **Data Processor** means any person, other than an employee of the Council, who processes data on behalf of the data controller, e.g. someone contracted to the Council to deal with documents containing personal data.

2.4 **Data subject** is the individual about whom personal data is held.

2.5 **Personal Data** means data about a living individual who can be identified from that information (or from that and other information in the possession of the data controller). This includes an expression of opinion about the individual, and any indication of the intentions of the data controller or any other in respect of that individual.

2.6 **Sensitive Personal Data** means personal data consisting of information as to:-

- racial or ethnic origin of the data subject
- his/her political opinion
- his or her religious beliefs or other beliefs of a similar nature
- whether he or she is a member of a trade union
- his or her physical or mental health or condition
- his or her sexual life
- the commission or alleged commission by him or her of an offence
- any proceedings for any offence committed or alleged to have been committed by him or her, the disposal of such proceedings or the sentence of any court in such proceedings

2.7 **Processing** is very widely drawn and means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including:-

- organisation, adaptation or alteration
- retrieval, consultation or use of,
- dissemination, disclosure or otherwise making available
- combination, blocking, erasure or destruction of the information or data

2.8 **Relevant Filing System** means any information held manually in an organised structure either by reference to individuals or other criteria such that specific information about a particular individual is readily accessible.

2.9 **Special Purposes** means any one or more of the following ie journalistic, artistic or literary.

3.0 Principles

The Data Protection Act 1998 contains 8 governing Principles relating to the collection, use, processing, and disclosure of data, and the rights of data subjects to have access to personal data concerning themselves. These Principles are:-

1 Personal data shall be processed fairly and lawfully and, in particular shall not be processed unless one of the conditions in Schedule 2 of the Act is met. These can be summarised as: where the individual has given consent; where the processing is necessary: for any contract, legal obligation, to protect the vital interests of the individual, or in the interests of justice and in the case of sensitive personal data at least one of the conditions in Schedule 3 of the Act is also met. The Schedule 3 conditions can be summarised as explicit consent, or where necessary for: employment obligations, vital interests, non-profit associations, manifestly made public, legal proceedings, administration of justice, medical purposes, ethnic monitoring

2 Personal data shall be obtained only for one or more specified and lawful purpose and shall not be further processed in any manner incompatible with that purpose or those purposes

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

4 Personal data shall be accurate and, where necessary, kept up to date

5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes

6 Personal data shall be processed in accordance with the rights of the data subject under this act (this includes the rights of subjects to access the data and to correct it)

7Appropriate technical and organisation measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (this relates to data security)

8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

These principles are regarded as the **minimum standards** of practice for any organisation with respect to personal data. Copies of the "Guidelines to the Data Protection Act", which illustrate these 8 principles are available from Sylvia Smith the Snr. Admin & Electoral Services Officer (extension 5031).

4.0 Policy

The Council Supports the objectives of the Data Protection Act 1998. This policy is intended to maintain the confidentiality of personal data held or processed either on computer, in manual files or otherwise and to increase the access given to individuals to information relating to them.

The Policy links to the other Council policies and documents for example:-

- ICT and Data Security Policy
- Retention and Disposal Schedule
- The Council's Constitution

- Code of Conduct
- Human Resources Policies
- Use of Internet & Email
- HIV and Aids Policy

It also links to the information sharing protocol with the Police Authority and to other initiatives under the Crime and Disorder Act 1998. There are a number of procedures underpinning this policy and guidance notes to supplement this policy for example:-

- Subject Access
- Registration/Notification
- New Systems
- Disclosures

4.1 External and Internal Registration/Notification

The Council will have an external notification (registration) with the Information Commissioner which will be supplemented by an **internal register of sources and disclosures.**

4.2 Amount of data to be held

The Council will hold the minimum personal data necessary to enable it to perform its functions. The data will be erased once the need to hold it has passed. Every effort will be made to ensure that data is accurate and up to date, and that inaccuracies are corrected quickly.

4.3 Subject Access

The Council will provide to any individual who requests it, in a specified manner, a reply stating whether or not the Council holds personal data about that individual. A written copy, in clear language, of the current data held, will be given. A fee of £10 will be charged for this service.

4.4 Public Registers

The Council maintains a number of public registers that contain personal data or data that could be used to identify individuals of these are examples set out in Appendix 1. Strict compliance with the legislation giving rights of access will be used in all cases.

4.5 Disclosures

Disclosures of information must be in accordance with the provisions of the Act, the Council's registration/notification and the internal register of sources and disclosures. The Council has a duty to disclose certain data to public authorities such as the Inland Revenue, Customs and Excise and Benefits agency this will be done in accordance with the statutory and other requirements.

Disclosure within the authority either to Council officers or elected members will be on the basis of a need to know this will be judged when a request for information is made. The minimum of personal data will be made generally available.

4.6 System Design

The Council intends that personal data must be treated as confidential. Computer and other systems will be designed to comply with the Principles of the Data Protection Act so that access to personal data should be restricted to identifiable system users.

4.7 Training

It is the aim of the Council that all appropriate staff will be properly trained, fully informed of their obligations under the Act and aware of their personal liabilities.

4.8 Disciplinary Action

The Council expects all of its staff and members to comply fully with this Policy and the Principles of the Data Protection legislation. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures following from this policy.

5.0 Responsibilities

Overall responsibility for the efficient administration of the Data Protection legislation lies with the **Council** and is exercised by the Cabinet.

5.1 Managing Directors and Heads of Service

Day to day responsibility for administration and compliance with the act is delegated to the Managing Directors and Heads of Service , for compliance with the Act's provisions within their respective areas of authority. Within each Service, Data Protection Link Officers may be appointed to undertake administration of data protection and to assist in compliance with the requirements of the legislation on behalf of the Managing Directors and Heads of Service (the number of Data Protection Link Officers in each Service will be a matter for the Heads of Service to determine).

5.2 Data Protection Officer (Snr. Admin & Electoral Services Officer)

It is the responsibility of the Data Protection Officer to assist the Council to ensure compliance with this policy, to specify the procedures to be adopted and to co-ordinate the activities of the designated Link Officers.

The main duties of the Data Protection Officer are:-

- maintenance of the Council's external registration/notification under the Act, and to act as liaison officer with the Information Commissioner
- development, updating and publication of data protection procedures for the Council.
- maintenance of the internal register of sources and disclosures and in association with the internal Audit Section to audit data protection procedures and practices.
- initial contact point for subject access requests.

- in conjunction with Human Resources , provision of education and training seminars regarding data protection issues

5.3 Head of ICT Service (WLBC)

The main duties of the Head of ICT are to:-

- Develop and enforce the ICT and Data Security Policy

5.4 Data Protection Link Officers

The Data Protection Link Officers are responsible to the Managing Directors and Heads of Service for:-

- liaison with the Data Protection Officer on all matters concerning administration of the Act

- working with the Managing Directors and Heads of Service to ensure compliance with the notification (registration) particulars in respect of systems within the Service;

- working with the Service Managers to ensure awareness of the Act within the Service, and to ensure that the control and handling of personal data within the Service does not contravene the Data Protection Principles or Council procedures.

- assisting the Data Protection Officer in the collation and validation of external and internal registration particulars relevant to the Service, and advising the Data Protection Officer of any planned changes to the registration particulars

- assisting in the response to access requests from data subjects.

5.5 Officers and Members

In addition to the formal responsibilities outlined above, all officers and members have a duty to observe the Principles of the Act and the procedures referred to in this document.

Individuals who do not handle personal data as part of their normal work have a responsibility to ensure that any personal data they see or hear goes no further. This includes personal data and information extracted from such data, thus, for example, unauthorised disclosure of data might occur by passing information over the telephone, communicating information contained on a computer print-out or even inadvertently by reading a computer screen.

Disciplinary action may result if the Data Protection Principles or procedures outlined in this document are breached.

Sources of Reference

Data Protection Act, 1984
Data Protection Act, 1998
European Union Data Protection Directive (95/46/EC)

Appendix 1

Examples of Publicly available information that could be used to identify individuals

Elections
Representation of the Peoples Act 2000
Register of persons who are eligible to vote in elections

Returns or declarations and accompanying documents relating to election expenses sent by a candidate of a parliamentary or local government election to the Council

Members Allowances
The Local Authority (Members' Allowances) Regulations 1991

Records of payments made to elected members are open to inspection by local government electors for the area. Additionally, the authority must publish within its own area details of the total sums paid under the scheme.

Committee Minutes Reports etc
Local Government Act 1972

Allows access to agendas and reports of committees and subcommittees. Minutes are also available

Taxis and Private Hire Vehicles
Town Police Clauses Act 1847
Local Government (Miscellaneous Provisions) Act 1976

Register containing information about owners and drivers of taxis and drivers of private hire vehicles.

AGENDA ITEM: 10

AUDIT AND GOVERNANCE:
29th January 2013

Report of: Borough Treasurer

Relevant Managing Director: Managing Director (People and Places)

Contact: Marc Taylor (Extn. 5092)
(E-mail: Marc.Taylor@westlancs.gov.uk)

SUBJECT: **ANNUAL AUDIT LETTER 2011/12 AND PLANNED AUDIT FEE 2012/13**

Wards affected: Borough Wide

1.0 PURPOSE OF THE REPORT

1.1 To consider the Audit Commission's Annual Audit Letter 2011/12 and details of Grant Thornton's planned audit fee for 2012/13.

2.0 RECOMMENDATION

2.1 That the Letters be considered and that any questions on them be raised with the External Auditors at the meeting.

3.0 BACKGROUND

3.1 Each year our External Auditors produce an Annual Audit Letter. This Letter provides an overall summary of the auditor's assessment of the Council, based on all of the work that they have undertaken. In addition each year our External Auditors provide details on their fee levels for the next year's audit.

3.2 The Audit Commission have been our external auditors for many years, but from November 2012 Grant Thornton have taken over this responsibility. Consequently the Annual Audit Letter, which related to the 2011-12 accounts and was issued in October 2012, was written by the Audit Commission. However the planned audit fee letter which relates to the 2012-13 audit and was issued in November 2012, has been produced by Grant Thornton. These letters are included in the appendices to these reports. While the bodies providing our external audit service have changed, the staff have remained the same, as they have transferred from the Audit Commission to Grant Thornton.

4.0 CURRENT ISSUES

4.1 The Annual Audit Letter provides the Council with a clean bill of health from a financial perspective. No significant issues were identified during the audit of the Statement of Accounts and the Letter concludes that the Council has proper arrangements in place to secure value for money.

4.2 The planned audit fees for 2012/13 represent a 40% reduction compared to costs in previous years. This saving has been included in the Major Service Review process and has been built into the budget for the next financial year.

4.3 Our external auditors will be attending the meeting and will be able to answer any questions that Members may have on the letters or on the new audit arrangements.

5.0 SUSTAINABILITY IMPLICATIONS/COMMUNITY STRATEGY

5.1 There are no significant sustainability impacts associated with this report and, in particular, no significant impact on crime and disorder. The report has no significant links with the Sustainable Community Strategy.

6.0 RISK ASSESSMENT

6.1 The Annual Audit Letter is an integral part of the Council's internal control framework and provides assurance to Members that the Council is operating effectively.

Background Documents

There are no background documents (as defined in Section 100D(5) of the Local Government Act 1972) to this Report.

Equality Impact Assessment

The decision does not have any direct impact on members of the public, employees, elected members and / or stakeholders. Therefore no Equality Impact Assessment is required.

Appendix

Appendix A - Audit Commission Annual Audit Letter 2011/12

Appendix B – Grant Thornton Planned Audit Fee for 2012/13

3 October 2012

The Joint Managing Directors
West Lancashire Borough Council
Council Offices
52 Derby Street
Ormskirk L39 2DF

Direct line 0844 798 7041
Email k-murray@audit-commission.gov.uk

Dear Gill and Kim,

West Lancashire Borough Council Annual Audit Letter 2011/12

I am pleased to submit my Annual Audit Letter which summarises my 2011/12 audit of West Lancashire Borough Council.

Financial statements

On 25 September 2012 I presented my Annual Governance Report (AGR) to the Audit and Governance Committee outlining the findings of my audit of the Council's 2011/12 financial statements. I will not replicate those findings in this letter.

Following the Audit and Assurance Committee, on 26 September 2012, I:

- issued an unqualified opinion on the Authority's 2011/12 financial statements included in the Council's Statement of Accounts;
- concluded that you have made proper arrangements to secure economy, efficiency and effectiveness in your use of resources; and
- certified completion of the audit.

Closing remarks

While this has been another challenging year for the Council I wish to thank the finance staff for their positive and constructive approach throughout the period. I also wish to thank senior management and the Audit and Governance Committee for their support and co-operation during the audit.

Please can you ensure that a copy of this letter is circulated to all Members.

Yours sincerely

Karen Murray
District Auditor

Marc Taylor
Borough Treasurer
West Lancashire Borough Council
52 Derby Street
Ormskirk
West Lancashire
L39 2DF

Grant Thornton UK LLP
4 Hardman Square
Spinningfields
Manchester M3 3EB

T +44 (0)161 953 6900
F +44 (0)161 953 6901
www.grant-thornton.co.uk

23 November 2012

Dear Marc

Planned audit fee for 2012/13

We are delighted to have been appointed by the Audit Commission as auditors to the Council and look forward to providing you with a high quality external audit service for at least the next five years. We look forward to developing our relationship with you over the coming months, ensuring that you receive the quality of external audit you expect and have access to a broad range of specialist skills where you would like our support.

The Audit Commission has set its proposed work programme and scales of fees for 2012/13. In this letter we set out details of the audit fee for the Council along with the scope and timing of our work and details of our team.

Scale fee

The Audit Commission defines the scale audit fee as "the fee required by auditors to carry out the work necessary to meet their statutory responsibilities in accordance with the Code of Audit Practice. It represents the best estimate of the fee required to complete an audit where the audited body has no significant audit risks and it has in place a sound control environment that ensures the auditor is provided with complete and materially accurate financial statements with supporting working papers within agreed timeframes."

For 2012/13, the Commission has independently set the scale fee for all bodies. The Council's scale fee for 2012/13 is £57,428. which compares to the audit fee of £95,713 for 2011/12, a reduction of 40%.

Further details of the work programme and individual scale fees for all audited bodies are set out on the Audit Commission's website at: www.audit-commission.gov.uk/scaleoffees1213.

The audit planning process for 2012/13, including the risk assessment, will continue as the year progresses and fees will be reviewed and updated as necessary as our work progresses.

Scope of the audit fee

Our fee is based on the risk based approach to audit planning as set out in the Code of Audit Practice and work mandated by the Audit Commission for 2012/13. It covers:

- our audit of your financial statements
- our work to reach a conclusion on the economy, efficiency and effectiveness in your use of

resources (the value for money conclusion)
- our work on your whole of government accounts return.

Value for money conclusion

Under the Audit Commission Act, we must be satisfied that the Council has adequate arrangements in place to secure economy, efficiency and effectiveness in its use of resources, focusing on the arrangements for:

- securing financial resilience; and
- prioritising resources within tighter budgets.

We undertake a risk assessment to identify any significant risks which we will need to address before reaching our value for money conclusion. We will assess the Council's financial resilience as part of our work on the VFM conclusion and a separate report of our findings will be provided.

Our planning to date has not identified any additional work which we are required to undertake to support our VFM conclusion. We will continue to assess the Council/Authority's arrangements and discuss any additional work required during the year.

Certification of grant claims and returns

The Audit Commission has replaced the previous schedule of hourly rates for certification work with a composite indicative fee. This composite fee, which is set by the Audit Commission, is based on actual 2010/11 fees adjusted to reflect a reduction in the number of schemes which require auditor certification and incorporating a 40% fee reduction. The composite indicative fee grant certification for the Council is £17,400.

Billing schedule

Our fees are billed quarterly in advance. Given the timing of our appointment we will raise a bill for two quarters in December 2012 with normal quarterly billing thereafter. Our fees will be billed as follows:

Main Audit fee	**£**
December 2012	28,714
March 2013	14,357
June 2013	14,357
Grant Certification	
June 2013	17,400
Total	**78,828**

Outline audit timetable

We will undertake our audit planning and interim audit procedures in the first quarter of 2013. Upon completion of this phase of our work we will issue our detailed audit plan setting out our findings and details of our audit approach. Our final accounts audit and work on the VFM conclusion will be completed in September 2013 alongside our work on the whole of government accounts.

Phase of work	Timing	Outputs	Comments
Audit planning and interim audit	Jan – Mar 2013	Audit plan	The plan summarises the findings of our audit planning and our approach to the audit of the Council's accounts and VFM.
Final accounts audit	Aug - Sept 2013	Report to those charged with governance	This report will set out the findings of our accounts audit and VFM work for the consideration of those charged with governance.
VFM conclusion	Jun - Sept 2013	Report to those charged with governance	As above
Financial resilience	Jun - Sept 2013	Financial resilience report	Report summarising the outcome of our work.
Whole of government accounts	September 2013	Opinion on the WGA return	This work will be completed alongside the accounts audit.
Annual audit letter	October 2013	Annual audit letter to the Council	The letter will summarise the findings of all aspects of our work.
Grant certification	Jun - Dec 2013	Grant certification report	A report summarising the findings of our grant certification work

Our team

The key members of the audit team for 2012/13 remain unchanged:

	Name	Phone Number	E-mail
Engagement Lead	Karen Murray	0161 234 6364	Karen.L.Murray@uk.gt.com
Engagement Manager	Claire Deegan	0161 214 6393	Claire.Deegan@uk.gt.com
Audit Executive	Paul Thompson	0161 234 6348	Paul.A.Thompson@uk.gt.com

Additional work

The scale fee excludes any work requested by the Council that we may agree to undertake outside of our Code audit. Each additional piece of work will be separately agreed and a detailed project specification and fee agreed with the Council.

Quality assurance

We are committed to providing you with a high quality service. If you are in any way dissatisfied, or would like to discuss how we can improve our service, please contact me in

the first instance. Alternatively you may wish to contact Sarah Howard, our Head of Public Sector Assurance on sarah.howard@uk.gt.com.

Yours sincerely

Karen Murray

For Grant Thornton UK LLP

AGENDA ITEM: 12

AUDIT AND GOVERNANCE COMMITTEE:
29 January 2013

CABINET:
19th March 2013

Report of: Borough Treasurer

Relevant Managing Director: Managing Director (People and Places)

Contact for further information: Marc Taylor (Extn. 5092)
(E-mail: marc.taylor@westlancs.gov.uk)

SUBJECT: REVIEW OF ANTI-MONEY LAUNDERING POLICY

Wards affected: Borough wide

1.0 PURPOSE OF THE REPORT

1.1 To set out the results of a review of the Council's Anti-Money Laundering Policy and Guidance and Procedure Notes.

2.0 RECOMMENDATIONS

2.1 That the updated Anti-Money Laundering Policy and Guidance and Procedure Notes, as set out in Appendix 1 and 2 to this report, be endorsed for agreement.

3.0 BACKGROUND

3.1 An Anti-Money Laundering Policy was first introduced in 2005 in response to new legislation set out in the Money Laundering Regulations 2003 which made public authorities more accountable for monitoring and detecting money laundering activities.

3.2 In 2010 a comprehensive review of these documents was undertaken leading to changes in the format of the policy and new guidance in the areas relating to 'failure to disclose' and 'tipping off'.

4.0 THE UPDATED POLICY

4.1 This latest review has focused on ensuring that the documents are still up to date with legislation, in line with best practice and accurate in terms of Council structure and Officer titles. This review has been competed and has established that the policy and procedures continue to meet best practice requirements.

4.2 The documents have been updated with the correct terminology following the change to the Managing Director structure in terms of having Services rather than Divisions.

4.3 The one area of note is that the responsibility for Deputy Money Laundering Reporting Officer has now been assigned to the Assistant Solicitor rather than the Borough Solicitor.

5.0 CURRENT POSITION

5.1 The Anti-Money Laundering Policy and Guidance and Procedure Notes have worked effectively since their inception but regular reviews are required to ensure the documents are still fit for purpose.

5.2 The Money Laundering Reporting Officer arrangements work effectively and this Officer – the Internal Audit Manager – along with his newly assigned Deputy are kept abreast of all current developments in money laundering and are, of course, the first officers to be made aware of any suspicious activities.

5.3 Due to the nature of the services provided by the Council instances of suspected money laundering are unlikely to arise, but there is a need to maintain the profile of this issue. Consequently, the Policy and Guidance Notes will be re-circulated to all staff following committee approval and further training offered where required.

6.0 BEST PRACTICE AND GUIDANCE

6.1 The Council's money laundering documentation take account of the guidance set out in the CIPFA best practice document 'Combating Financial Crime: Further guidance on anti-money laundering for public services organisations 2009'.

7.0 SUSTAINABILITY IMPLICATIONS/COMMUNITY STRATEGY

7.1 There are no significant sustainability implications associated with this report and the report has no significant links with the Sustainability Community Strategy

8.0 FINANCIAL AND RESOURCE IMPLICATIONS

8.1 The operation of the money laundering framework will be accommodated within existing resources.

9.0 RISK ASSESSMENT

9.1 Legislation requires that the Council has adequate procedures in place for the reporting of suspected money laundering activities. Failure to do so would be in breach of this legislation and lack of knowledge in this area could lead staff to inadvertently commit offences. Both would jeopardise the good reputation of the Council.

Background Documents

CIPFA 'Combating financial crime: Further guidance on anti-money laundering for public services organisations 2009'

Equality Impact Assessment

The decision does not have any direct impact on members of the public, employees, elected members and / or stakeholders. Therefore no Equality Impact Assessment is required.

Appendices

Appendix 1 – Anti-Money Laundering Policy
Appendix 2 – Anti-Money Laundering Guidance and Procedures

WEST LANCASHIRE BOROUGH COUNCIL

ANTI-MONEY LAUNDERING POLICY

1.0 INTRODUCTION

1.1 The Proceeds of Crime 2002 Act, the Terrorist Act 2000 and the Money Laundering Regulations 2007 broadly define money laundering and the range of activities covered by the statutory framework. Obligations impact on certain areas of local authority business and require local authorities to establish internal procedures to prevent the use of their services for money laundering. It is, therefore, good practice to have a robust Policy in place and promote staff awareness of potential money laundering activity.

2.0 SCOPE OF THE POLICY

2.1 This Policy applies to all employees of the Council and aims to maintain the high standards of conduct which currently exist within the Council by preventing criminal activity through money laundering. The Policy sets out the procedures that must be followed (for example the reporting of suspicions of money laundering activity) to enable the Council and its officers to comply with their legal obligations.

2.2 Further information is set out in the accompanying Anti-Money Laundering Guidance Note and Procedures. Both sit alongside the Council's Whistleblowing Code and Anti-Fraud, Bribery and Corruption Policy.

2.3 Failure by a member of staff to comply with the procedures set out in this Policy may lead to disciplinary action being taken against them. Any disciplinary action will be dealt with in accordance with the Council's Disciplinary Policy and Procedure. It should also be noted that in certain instances officers might themselves become criminally liable for breach of the 2000 Act, 2002 Act and the 2007 Regulations.

3.0 WHAT IS MONEY LAUNDERING?

3.1 These are the primary money laundering offences and thus prohibited acts under the law:

- concealing, disguising, converting, transferring criminal property or removing it from the UK; or
- entering into or becoming concerned in an arrangement which you know or suspect facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person; or
- acquiring, using or possessing criminal property; or
- becoming concerned in an arrangement facilitating concealment, removal from the jurisdiction, transfer to nominees or any other retention or control of terrorist property.

3.2 Potentially any member of staff could be caught by the money laundering provisions if they suspect money laundering and either become involved with it in some way and/or do nothing about it. The Guidance Note and Procedures document gives practical examples. This Policy sets out how any concerns should be raised.

3.3 Whilst the risk to the Council of contravening the legislation is low, ***it is important that all employees are familiar with the legal responsibilities: serious criminal sanctions can be imposed for breaches of the legislation.***

4.0 WHAT ARE THE OBLIGATIONS ON THE COUNCIL?

4.1 The law requires those organisations in the 'regulated sector' and conducting 'relevant business' to

- appoint a Money Laundering Reporting Officer ("MLRO") to receive disclosures from employees of money laundering activity (their own or anyone else's);
- implement a procedure to enable the reporting of suspicions of money laundering;
- maintain client identification and record keeping procedures.

4.2 It is considered that the Council does not fall within the regulated sector nor does it conduct relevant business. However it is good practice, and will aid the Council's compliance with the wider requirements of the relevant legislation if it adopts policies and procedures which are in line with the requirements identified in the bullet points above.

4.3 All staff are required to comply with the reporting procedure set out in section 6 below to ensure consistency throughout the organisation and avoid inadvertent offences being committed.

4.4 The following sections of this Policy provide further detail about the requirements listed in paragraph 4.1 to the extent that they are relevant to the Council.

5.0 THE MONEY LAUNDERING REPORTING OFFICER

5.1 The officer nominated to receive disclosures about money laundering activity within the Council is the Internal Audit Manager, Mike Coysh (MLRO) (i). He can be contacted as follows:

Mike Coysh
Internal Audit Manager
52 Derby Street
Ormskirk

Telephone: 01695 712603 (internal 2603)

5.2 In the absence of the MLRO, the ~~Legal Services Manager~~Assistant Solicitor, ~~Terry Broderick~~Michael Hynes, is authorised to deputise for him. He can be contacted at the 52 Derby Street offices address or on ~~telephone number 01695 585001(direct line)~~extension 5522.

(i) Note, this is not a formal appointment under section 337 or 338 of the 2002 Act

6.0 DISCLOSURE PROCEDURE

Reporting to the Money Laundering Reporting Officer

6.1 Where you know or suspect that money laundering activity is taking/has taken place, or become concerned that your involvement in a matter may amount to a prohibited act under the legislation, you must disclose this as soon as practicable to the MLRO. The disclosure should be within "hours" of the information coming to your attention, not weeks or months later. Whilst failure to disclose is no longer an offence for public authorities under the 2007 regulations, it is in your best interest and the interests of the Council to do so.

6.2 Your disclosure should be made to the MLRO using the proforma report ~~attached at Appendix 1~~set out in the Guidance Notes and Procedures. The report must include as much detail as possible, for example:

- Full details of the people involved (including yourself, if relevant), e.g. name, date of birth, address, company names, directorships, phone numbers, etc;
- Full details of the nature of their/your involvement;
  - If you are concerned that your involvement in the transaction would amount to a prohibited act under the Proceeds of crime Act, then your report must include all relevant details, as you will need consent from the Serious Organised Crime Agency (SOCA), via the MLRO, to take any further part in the transaction - this is the case even if the client gives instructions for the matter to proceed before such consent is given.
  - You should therefore make it clear in the report if such consent is required and clarify whether there are any deadlines for giving such consent, e.g. a completion date or court deadline;
- The types of money laundering activity involved:
  - if possible, cite the section number(s) under which the report is being made
- The dates of such activities, including:
  - Whether the transactions have happened, are ongoing or are imminent;
    Where they took place;
    How they were undertaken;
    The (likely) amount of money/assets involved;
    Why, exactly, you are suspicious – SOCA will require full reasons;

along with any other available information to enable the MLRO to make a sound judgement as to whether there are reasonable grounds for knowledge or suspicion of money laundering and to enable him to prepare his report to SOCA, where appropriate. You should also enclose copies of any relevant supporting documentation.

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

6.4 Similarly, **at no time and under no circumstances should you voice any suspicions** to the person(s) whom you suspect of money laundering, even if SOCA has given consent to a particular transaction proceeding, without the specific consent of the MLRO. 'Tipping off' is no longer an offence under the 2007 regulations for public authorities, however to do so may jeopardise the investigation

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

Consideration of the disclosure by the Money Laundering Reporting Officer

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

6.7 The MLRO will consider the report and any other available internal information he thinks relevant e.g.:

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

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

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

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

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

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

6.9.2 In cases where legal professional privilege may apply, the MLRO must liaise with the legal adviser to decide whether there is a reasonable excuse for not reporting the matter to SOCA.

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

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

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

7.0 CLIENT IDENTIFICATION PROCEDURE

7.1 The client identification procedure – putting in place formal procedures for evidencing the identity of those they do business with under the 2007 regulations - is only required, under the regulations, by those engaging in specific areas of Council activity. It is essential, however, for all staff to ensure they are constantly alert to potentially suspicious circumstances, for example, situations where funds flow through the Council from a source with which it is unfamiliar.

7.2 In particular, if the Council is forming a new business relationship, and/or is considering undertaking a significant one-off transaction, officers must ensure that their own ~~divisional~~ service procedures satisfy the requirements of the Client Identification Procedure before any business is undertaken for that client. This will be especially true if the parties concerned are not physically present for identification purposes and to situations where they may be acting for absent third parties. Satisfactory evidence of the identity of the prospective client should be obtained beforehand. For advice on appropriate and acceptable identification documents and any record keeping requirements, contact the MLRO.

8.0 CONCLUSION

8.1 The legislative requirements concerning anti-money laundering procedures are lengthy and complex. This Policy has been written so as to enable the Council to meet the legal requirements in a way which is proportionate to the very low risk to the Council of contravening the legislation.

8.2 Should you have any concerns whatsoever regarding any transactions then you should contact the MLRO.

WEST LANCASHIRE BOROUGH COUNCIL – ANTI MONEY LAUNDERING POLICY – APPENDIX 1

CONFIDENTIAL

Report to Money Laundering Reporting Officer

re money laundering activity

To: Mike Coysh**, Money Laundering Reporting Officer**

From: ……
[insert name of employee]

~~Division~~Service: …….. Ext/Tel No:……..
[insert post title]

Name(s) and address(es) of person(s) involved: (if a company/public body please include details of nature of business)

Nature, value and timing of activity involved: (please include full details e.g. what, when, where, how. Continue on separate sheet if necessary)

Nature of suspicions regarding such activity:
(please continue on separate sheet if necessary)

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

If yes, please include details below:

Have you discussed your suspicions with anyone else? ☐ Yes ☐ No
(please tick relevant box)

If yes, please specify below, explaining why such discussion was necessary:

Have you consulted any supervisory body for guidance re money laundering? (e.g. the Law Society) (please tick relevant box) ☐ Yes ☐ No

If yes, please specify below:

Do you feel you have a reasonable excuse for not disclosing the Matter to the NCIS? (e.g. are you a lawyer and wish to claim legal professional privilege?) (please tick the relevant box) ☐ Yes ☐ No

If yes, please set out full details below:

Are you involved in a transaction which might be a prohibited act under Sections 327-329 of the Act and which requires appropriate consent from the NCIS? (please tick relvant box) ☐ Yes ☐ No

If yes, please enclose details in the box below:

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

Signed:……. Dated:……

Please do not discuss the content of this report with anyone you believe to be involved in the suspected money laundering activity described.

THE FOLLOWING PART OF THIS FORM IS FOR COMPLETION BY THE MLRO

Date report received: ……...

Date receipt of report acknowledged: ……..

CONSIDERATION OF DISCLOSURE:

Action Plan:

OUTCOME OF CONSIDERATION OF DISCLOSURE:

Are there reasonable grounds for suspecting money laundering activity?

If there are reasonable grounds for suspicion, will a report be made to the NCIS? (please tick relevant box) ☐ Yes ☐ No

If yes, please confirm date of report to NCIS: ……
and complete the box below:

Details of liaison with the NCIS regarding the report:

Notice period: ……. to …….

Moratorium period: …….to ……...

Is consent required from the NCIS to any ongoing or imminent transactions which would otherwise be prohibited acts? ☐ Yes ☐ No

If yes, please confirm full details in the box below:

Date consent received from NCIS: ……
Date consent given by you to employee: ……

If there are reasonable grounds to suspect money laundering, but you do not intend to report the matter to the NCIS, please set out below the reason(s) for non-disclosure:

Date consent given by you to employee for any prohibited act transactions to proceed: …….

Other relevant information:

Signed: …….. Dated: ……..

THIS REPORT TO BE RETAINED FOR AT LEAST FIVE YEARS

WEST LANCASHIRE BOROUGH COUNCIL

GUIDANCE NOTE & PROCEDURES

RE THE ANTI-MONEY LAUNDERING POLICY

INTRODUCTION

Historically, legislation seeking to prevent the laundering of the proceeds of criminal activity was aimed at professionals in the financial and investment sector, however it was subsequently recognised that those involved in criminal conduct were able to "clean" the proceeds of crime through a wider range of businesses and professional activities.

New obligations in respect of money laundering were therefore imposed by the Proceeds of Crime 2002 Act, the Terrorist Act 2000 and the Money Laundering Regulations 2003, which were replaced by the Money Laundering Regulations 2007. These broadly define money laundering and the range of activities covered by the statutory control framework, in particular the duty to report suspicions of money laundering.

As a result, certain areas of the Council's business are subject to the legislative controls and the Council is required to establish guidance and procedures designed to prevent the use of its services for money laundering. All staff should be aware of the content.

The Policy and this Guidance Note and Procedures document will be sufficient for most staff in providing detail on the legal requirements and practical help, however, for staff in areas which have a higher risk of being exposed to money laundering activities, additional training will be provided.

All members of staff are required to comply with the Council's Anti-Money Laundering Policy in terms of reporting concerns re money laundering; this will ensure consistency throughout the Council and avoid inadvertent offences being committed.

THE OFFENCES

Under the legislation there are two main types of offences which may be committed: money laundering offences and failure to report money laundering offences.

Money laundering now goes beyond the transformation of the proceeds of crime into apparently legitimate money/assets: it now covers a range of activities (which do not necessarily need to involve money or laundering) regarding the proceeds of crime. It is technically defined as any act constituting:

- an offence under the 2002 Act i.e.:

    - □ concealing, disguising, converting, transferring criminal property (i) or removing it from the UK; or
    - □ entering into or becoming concerned in an arrangement which a person knows or suspects facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person; or

- □ acquiring, using or possessing criminal property (unless there was adequate consideration);
- □ an attempt, conspiracy or incitement to commit such an offence; or
- □ aiding, abetting, counselling or procuring such an offence; and

- an offence under the Terrorist Act 2000, namely becoming concerned in an arrangement facilitating concealment, removal from the jurisdiction, transfer to nominees or any other retention or control of terrorist property (ii).

Note also that any attempt, conspiracy or incitement to commit any of the offences noted above; or aiding, abetting, counselling or procuring such offences will also be the subject of a criminal sanction.

It is likely that the law will treat you as knowing that which you do know or which is obvious, or which an honest and reasonable person would have known given the circumstances and the information you have. Consequently if you deliberately shut your mind to the obvious, this will not absolve you of your responsibilities under the legislation.

Although you do not need to have actual evidence that money laundering is taking place, mere speculation or gossip is unlikely to be sufficient to give rise to knowledge or suspicion that it is.

The legislation goes beyond major drug money laundering operations, terrorism and serious crime to cover the proceeds of potentially any crime, no matter how minor and irrespective of the size of the benefit gained.

The broad definition of money laundering means that potentially anybody (and therefore any Council employee, irrespective of what sort of Council business they are undertaking) could contravene the money laundering offences if they become aware of, or suspect the existence of criminal or terrorist property, and continue to be involved in the matter without reporting their concerns.

The money laundering regime is far reaching and does not just relate to the activities of organised crime, offences under POCA could also apply to being complicit in crimes relating to falsification of benefit claims, benefiting from non-compliance of conditions attached to a grant and facilitating employment upon which tax is not paid.

The Council has appointed the Audit Manager, Mike Coysh, as its Money Laundering Reporting Officer (MLRO) to receive reports from employees of suspected money laundering activity (iii).

(i) “criminal property” is widely defined: it is property representing a person’s benefit from criminal conduct where you know or suspect that that is the case. It includes all property (situated in the UK or abroad) real or personal, including money, and also includes an interest in land or a right in relation to property other than land.

(ii) “terrorist property” means money or other property which is likely to be used for the purposes of terrorism, proceeds of the commission of acts of terrorism, and acts carried out for the purposes of terrorism.

(iii) Note, this is not a formal appointment under section 337 or 338 of the 2002 Act

Examples of money laundering activity:

By way of example, consider the following hypothetical scenario:

> *A Housing Officer is assessing a service user's finances to calculate how much they should pay towards the cost of electrical goods, and then goes on to arrange for goods to be provided and charged for, in the course of which s/he becomes aware of, or suspects the existence of, criminal property.*

In this scenario the Housing Officer may commit an offence under section 328 by “being concerned in an arrangement” which s/he knows/suspects “facilitates the acquisition, retention, use or control of criminal property” if s/he does not report his/her concerns. Any lawyer involved could also be guilty of an offence if s/he assists in the transaction.

Any person found guilty of a money laundering offence is liable to imprisonment (maximum of 14 years), a fine or both; however an offence is not committed if the suspected money laundering activity is reported to the MLRO and, where necessary, official permission obtained to continue in the transaction.

Defences are available if, for example, the person:

- makes an 'authorised disclosure' under the 2002 Act to the Serious Organised Crime Agency (SOCA) or the MLRO and SOCA gives consent to continue with the transaction; such a disclosure will not be taken to breach any rule which would otherwise restrict that disclosure;
- intended to make such a disclosure but had a reasonable excuse for not doing so;
- acquired, used or possessed the property for adequate consideration.
- did not know and had no reasonable cause to suspect the arrangement related to terrorist property or criminal property as the case may be.

POSSIBLE SIGNS OF MONEY LAUNDERING

It is impossible to give a definitive list of ways in which to spot money laundering or how to decide whether to make a report to the MLRO. The following are types of risk factors which may, either alone or cumulatively with other factors, suggest the possibility of money laundering activity:

GENERAL

- A new client;
- A secretive client: e.g., refuses to provide requested information without a reasonable explanation;
- Concerns about the honesty, integrity, identity or location of a client;
- Illogical third party transactions: unnecessary routing or receipt of funds from third parties or through third party accounts;
- Involvement of an unconnected third party without logical reason or explanation;
- Payment of a substantial sum in cash (over £10,000);

- Overpayments by a client;
- Absence of an obvious legitimate source of the funds;
- Movement of funds overseas, particularly to a higher risk country or tax haven;
- Where, without reasonable explanation, the size, nature and frequency of transactions or instructions (or the size, location or type of a client) is out of line with normal expectations;
- A transaction without obvious legitimate purpose or which appears uneconomic, inefficient or irrational;
- The cancellation or reversal of an earlier transaction;
- Requests for release of client account details other than in the normal course of business;
- Companies and trusts: extensive use of corporate structures and trusts in circumstances where the client's needs are inconsistent with the use of such structures;
- Poor business records or internal accounting controls;
- A previous transaction for the same client which has been, or should have been, reported to the MLRO;

PROPERTY MATTERS

- Unusual property investment transactions if there is no apparent investment purpose or rationale;
- Instructions to receive and pay out money where there is no linked substantive property transaction involved (surrogate banking);
- Re property transactions, funds received for deposits or prior to completion from an unexpected source or where instructions are given for settlement funds to be paid to an unexpected destination;

Facts which tend to suggest that something odd is happening may be sufficient for a reasonable suspicion of money laundering to arise.

In short, the money laundering offences apply to your own actions and to matters in which you become involved. If you become aware that your involvement in a matter may amount to money laundering under the 2002 Act then you must discuss it with the MLRO and not take any further action until you have received, through the MLRO, the consent of SOCA. The failure to report money laundering obligations relate also to your knowledge or suspicions of others, through your work.

WHAT ARE MY RESPONSIBILITIES?

The Council's Anti-Money Laundering Policy makes it clear that all members of staff should report any concerns they may have of money laundering activity, irrespective of their area of work.

In relation to money laundering offences themselves, potentially any member of staff could breach the legislation if they knew or suspected money laundering and became involved with it in some way without reporting their concerns.

If you know or suspect, through the course of your work, that anyone is involved in any sort of criminal conduct then it is highly likely, given the wide definition of money laundering, that the client is also engaged in money laundering and a report to the

MLRO will be required. The value involved in the offence is irrelevant. If, for example, you reasonably suspect that someone has falsified their expenses claim, even if just by £1, then you would need to report that to the MLRO.

Do not voice any suspicions to the person(s) whom you suspect of money laundering or involve other officers/individuals. 'Tipping off' is no longer an offence under the 2007 regulations for public authorities, however to do so may jeopardise the investigation.

If you suspect a case of money laundering you should report the details immediately to the Council's Money Laundering Reporting Officer (MLRO) Mike Coysh (ext 2603) or in his absence the Deputy MLRO ~~Terry Broderick~~Michael Hynes (ext ~~5001~~5522). Such disclosures to the MLRO will be protected in that they will not be taken to breach any restriction on the disclosure of information.

The report should be made either by completing the proforma at Appendix 1 of the Anti-money Laundering Policy, or if you prefer, in a discussion.

You should still report your concerns, even if you believe someone else has already reported their suspicions of the same money laundering activity.

If you are in any doubt as to whether or not to file a report with the MLRO then you should err on the side of caution and do so. The MLRO will not refer the matter on to SOCA if there is no need.

CONSIDERATION OF DISCLOSURE REPORT BY MLRO

Where the MLRO receives a disclosure from a member of staff and concludes that there is actual/suspected money laundering taking place, or there are reasonable grounds to suspect so, then he must make a report as soon as practicable to SOCA on their standard report form and in the prescribed manner, unless he has a reasonable excuse for non-disclosure. Where relevant, the MLRO will also need to request appropriate consent from SOCA for any acts/transactions, which may otherwise amount to prohibited acts under the 2002 Act, to proceed.

The MLRO may receive appropriate consent from SOCA in the following ways:

- specific consent;
- no refusal of consent during the notice period (seven working days starting with the first working day after the MLRO makes the disclosure); or
- refusal of consent during the notice period but the moratorium period has expired (31 days starting with the day on which the MLRO receives notice of refusal of consent).

RELEVANT GUIDANCE

When considering any offence under the legislation, the Court will consider whether you followed any relevant guidance approved by the Treasury, a supervisory authority, or any other appropriate body which includes, for example, the Law Society, the Financial Services Authority, the Institute of Chartered Accountants in England and Wales and other such bodies. Such guidance is available for lawyers and accountants by their respective professional bodies.

CLIENT IDENTIFICATION PROCEDURE

The client identification procedure – putting in place formal procedures for evidencing the identity of those they do business with under the 2007 regulations - is only required,

under the regulations, by those engaging in specific areas of Council activity. It is essential, however, for all staff to ensure they are constantly alert to potentially suspicious circumstances, for example, situations where funds flow through the Council from a source with which it is unfamiliar.

In particular, if the Council is forming a new business relationship, and/or is considering undertaking a significant one-off transaction, officers must ensure that their own ~~divisional~~ service procedures satisfy the requirements of the Client Identification Procedure before any business is undertaken for that client. This will be especially true if the parties concerned are not physically present for identification purposes and to situations where they may be acting for absent third parties. Satisfactory evidence of the identity of the prospective client should be obtained beforehand. Further guidance can be obtained from the MLRO.

If you are undertaking work for a new client, then you may also wish to corroborate the details they provide/identity using any other sources available e.g.:

- check the organisation's website to confirm the identity of personnel, its business address and any other details;
- attend the client at their business address;
- search the telephone directory;
- ask the key contact officer to provide evidence of their personal identity and position within the organisation

CONCLUSION

Given the nature of what the Council does and who it can provide services for, instances of suspected money laundering are unlikely to arise very often, if at all; however we must be mindful of the legislative requirements, as failure to comply with them may render the Council and/or individuals liable to prosecution and will also severely affect the reputation of the Council if it were to be implicated in such activity.

Please take prompt and proper action if you have any suspicions and feel free to consult the MLRO at any time should you be concerned regarding a matter.

Resources used in connection with the preparation of the Anti-Money Laundering Policy and Guidance Note (and helpful reference points):

www.moneylaunderingreporting.co.uk
http://www.soca.gov.uk/
www.anti-moneylaundering.org
www.theclc.gov.uk
www.fowles.co.uk/MoneyLaundering.htm
www.hardwickecrime.co.uk/access/resources/articles/03031201
The Financial Services' Authority Handbook
The Law Society "Money Laundering: Guidance for Solicitors (Pilot – January 2004)"
"The Money Laundering Regulations" by Charles Ward (The Legal Executive Journal)

“I Spy” by Jon Robins (The Lawyer magazine)
“Secret Disservice” by Peter Caldwell (The Lawyer magazine 8.3.04)
“Property lawyers – are you ready?” by Vanessa France & Jonathan Mills (The Young Solicitors Group Mar/Apr 04)
CIPFA’s Combating financial crime. Further guidance on Anti-money laundering for Public Services Organisations 2009

AGENDA ITEM 13

Audit & Governance Committee Work Programme – 29 January 2012

Date	Training (commencing 6.30pm)	Reports
26 March 2013	Contract Procedure Rules	1. Internal Audit Plan 2013/14 2. Local Code of Governance 3. Treasury Management 4. Internal Audit Activities – Quarterly Update 5. Regulation of Investigatory Powers Act quarterly monitoring of use of powers. 6. Audit Standards 7. External Audit Report – Claims and Returns
June 2013	Financial Regulations	1. Annual Governance Statement 2. Statement of Accounts 3. Internal Audit Activities – Quarterly Update 4. Internal Audit Activities – Annual report 5. Regulation of Investigatory Powers Act quarterly monitoring of use of powers.
September 2013	Housing Self Financing	1. Annual Governance Report 2. Internal Audit Mid-Year Review 3. Approval of Statement of Accounts 4. Regulation of Investigatory Powers Act quarterly monitoring of use of powers 5. Annual Review - Anti-Fraud, Bribery and Corruption Policy 6. The Effectiveness of the Data Quality Protocol
January 2014	Basic Guide to Governance	1. Risk management Framework 2. Internal Audit Activities – Quarterly Update 3. Regulation of Investigatory Powers Act quarterly monitoring of use of powers

NOTE Additional reports will be added to the Work Programme once the arrangements with Grant Thornton are made clear.