Public Document Pack

Date: **10 June 2011**
Our ref: Cabinet/Agenda
Ask For: **Charles Hungwe**
Direct Dial: **(01843) 577186**
Email: **charles.hungwe@thanet.gov.uk**

thanet district council

CABINET

23 JUNE 2011

A meeting of the Cabinet will be held at **7.00 pm on Thursday, 23 June 2011** in the Council Chamber, Cecil Street, Margate, Kent.

Membership:

Councillor Bayford (Chairman); Councillors: Bruce, Moores, Wells and Wise

A G E N D A

Item No | Subject

1. **APOLOGIES FOR ABSENCE**

2. **DECLARATIONS OF INTEREST**

   To receive any declarations of interest. Members are advised to consider the extract from the Standard Board Code of Conduct for Members, which forms part of the Declaration of Interest Form at the back of this Agenda. If a Member declares an interest, they should complete that Form and hand it to the Officer clerking the meeting.

3. **MINUTES OF PREVIOUS MEETING** (Pages 1 - 2)

   To approve the summary of recommendations and decisions of the Cabinet meeting held on 28 April 2011, copy attached.

4. **CHAIRMAN'S REMARKS - PETITION TO COUNCIL - LAND MANAGEMENT ISSUES - DEVELOPMENT PROPOSALS IN HARTSDOWN PARK FROM MARGATE FOOTBALL CLUB**

5. **CONFIRMATION OF ARTICLE 4 DIRECTION** (Pages 3 - 6)

6. **HOMES AND COMMUNITIES AGENCY BID FOR NEW AFFORDABLE HOMES** (Pages 7 - 10)

7. **DATA PROTECTION ACT (1998) - POLICY & PROCEDURES** (Pages 11 - 58)

8. **ST JOHN'S LODGE, ST JOHN'S CEMETARY, MARGATE** (Pages 59 - 60)

9. **EXCLUSION OF PUBLIC AND PRESS** (Pages 61 - 62)

10. **COACH HOUSE, NORTHDOWN PARK** (Pages 63 - 66)

Declaration of Interest form - back of agenda

This page is intentionally left blank

CABINET

Minutes of the meeting held on 28 April 2011 at 7.00 pm in Council Chamber, Council Offices, Cecil Street, Margate, Kent.

Present: Councillor Robert W Bayford (Chairman); Councillors Latchford, Moores, Wells and Wise

In Attendance: Councillor D Green, C Hart, Mrs Johnston, King and R Nicholson

123. APOLOGIES FOR ABSENCE

There were no apologies received.

124. DECLARATIONS OF INTEREST

There were no declarations of interest.

125. MINUTES OF PREVIOUS MEETINGS

The minutes were agreed and signed by the Chairman.

126. COMMUNITY SAFETY PLAN 2011/12

The Community Safety Plan listed activities from the previous 12 months, gave four clear priorities and outlined actions that were due to take place within 2011/12.

Councillor Mrs Johnston spoke under Procedure Rule 24.1

Councillor Wells moved, Councillor Bayford seconded and Members agreed the following:

1. That the Thanet Community Safety Plan 2011-12 be endorsed as a worthwhile plan to take forward by responsible officers from Enforcement Services and Kent Police in 2011-12.

127. RECORD OF DECISION BY INDIVIDUAL CABINET MEMBER - THE NEWINGTON CENTRE RE-DEVELOPMENT

The report sought to update Cabinet that an individual Cabinet Member Decision had been made regarding the Re-development of Newington Centre.

Councillor R. Nicholson spoke under Procedure Rule 24.1

Councillor Wells moved, Councillor Bayford seconded and Members agreed to note the report.

128. RECORD OF DECISION BY INDIVIDUAL CABINET MEMBER - THE MARGATE HARBOUR ARM

The report sought to update Cabinet that an individual Cabinet Member Decision had been made regarding the Margate Harbour Arm.

Councillor Mrs Johnston spoke under Procedure Rule 24.1

Councillor Latchford moved, Councillor Bayford seconded and Members agreed to note the report.

129. EXCLUSION OF PUBLIC AND PRESS

Councillor Moores moved, Councillor Latchford seconded and Members agreed the following:

1. That the public and press be excluded from the meeting on agenda items 8 and 9 as they contain exempt information as defined in Paragraph 3 of Schedule 12A of the Local Government Act 1972 (as amended).

130. DREAMLAND, MARGATE

Councillor Bayford moved, Councillor Latchford and Members agreed the following:

1. Cabinet agreed that the report be received and noted;

2. Cabinet noted and approved the revised Land Acquisition and Delivery Strategy set out in Paragraphs 4.1 to 4.5 of the Officers' report;

3. Cabinet agreed that in the event that a Compulsory Purchase Order is made pursuant to Section 226 of the Town & Country Planning Act 1990 in respect of the Dreamland site under powers delegated by the Cabinet to the Director of Regeneration Services, any such Order be made by reference to the land shown shaded pink and edged red on the revised Plan at Annex 2 to the Officers' Report;

4. Cabinet adopted Scenario C as the most prudent approach to the CPO strategy in order to avoid the Council incurring future potential costs without the availability of external funding.

131. WESTCLIFFE HALL

Councillor Bayford moved, Councillor Latchford seconded and Members agreed the following:

1. That Cabinet is minded to agree the principles set out in the report; but requires more detailed financial appraisal before a final decision can be made and that the matter be deferred to the next Cabinet meeting when the full report would be available.

Meeting concluded : 7.27 pm

CONFIRMATION OF ARTICLE 4 DIRECTION

To: **Cabinet Meeting - 23 June 2011**

Portfolio: **Economic Development and Regeneration**

By: **Simon Thomas, Planning Manager**

Classification: **Unrestricted**

Summary: **For Members to decide whether to confirm the Article 4 Direction made on 3 February 2011 which would remove permitted development rights and require a planning application to be made by a person wishing to change the use of a dwelling-house to a House in Multiple Occupation for up to 6 unrelated people**

For Decision

1.0 Introduction and Background

1.1 Until 1 October 2010 planning permission was required for the change of use of a building including a dwelling-house to an House in Multiple Occupation (HMO). On 1 October 2010 the Government introduced new legislation. Now planning permission is not required for the change of use of a dwelling house to an HMO for up to 6 unrelated people.

1.2 The option exists for Councils to remove this right for parts of its District. This power lies within the existing provisions of Article 4 of the Town and Country Planning (General Permitted Development) Order 1995 (as amended). Under Article 4 a Direction may be made by a Local Planning Authority to remove permitted development rights and require a planning application to be made, in this case, by a person wishing to change the use of a dwelling-house to an HMO

1.3 The making of an Article 4 direction would not mean a blanket ban on HMO's, as it would remain open to an owner to apply for permission for HMO and no fee would be required for such application.

1.4 The principle of making an Article 4 Direction was agreed by Council in December 2010. However, in accordance with the Constitution for Thanet, responsibility for the decision to make an Article 4 Direction falls to the Cabinet. Under the constitution where a matter is urgent and cannot reasonably await the next meeting the relevant Portfolio holder can make a decision on behalf of the Cabinet, in consultation with the Leader, subject to the decision being reported to Cabinet as soon as practicable. As the Direction (if confirmed) cannot come into force for 12 months from the date of making, it is considered that the decision is urgent and cannot reasonably await the next ordinary meeting of the Cabinet.

1.5 In this case the Portfolio Holder made his decision to authorise the making of an Article 4 Direction on 3 February 2011. The Direction will come into force after 12 month of this date. However, in order for this to happen the Direction must be confirmed by the Cabinet within 6 months of it having been made. The Cabinet must

consider any representations made before deciding whether the Direction should be confirmed.

2.0 Justification for making an Article 4 Direction

2.1 The justification for making an Article 4 Direction to remove the right of owners to change the use of dwellings to HMO's across the District lies in the harm that would be caused as a result of a further increase in HMO's in Thanet which, because of the transient nature of the potential future occupiers of such accommodation and the inability of services in Thanet to meet their needs would cause demonstrable harm to the character of neighbourhoods affected by a proliferation of HMO's and to residential amenity by reason of noise, disturbance and parking issues.

2.2 There is a current policy in the Thanet Local Plan (H11) that regulates the changes of use of buildings to HMOs, and requires consideration to be given to the impacts of HMO's including the effect of the use in terms of noise and disturbance. The Cliftonville Development Plan Document, shows that the large number of small flats and HMO's, which are generally in poor condition and therefore cheap to rent correlates with the attraction of vulnerable people from outside of Thanet into this District

2.3 The Strategic Housing Market Assessment (SHMA) that has been carried out for the East Kent sub region, recommends *that the districts in the sub-region develop further policies to balance housing markets through intervening to maximise the potential of existing stock. Whilst the Core Strategy Preferred Options Consultation Document sets out the Council's* aims to achieve a balance in the type of housing stock comparable with the Kent average, as well as to protect the overall supply of family houses. These considerations also provide a justification for making a District wide Article 4 Direction.

3.0 Compensation Liability

3.1 The making of a Direction under Article 4 renders the Council liable to pay compensation to people who have applied and been refused permission or been granted permission with conditions. Under the planning system there is a general principle that once permission has been granted, either by a specific grant of planning permission or by means of a Development Order, the right to develop is guaranteed and can only be withdrawn upon payment of compensation.

3.2 However, the provisions of The Town and Country Planning (Compensation) (No.3) (England) Regulations 2010 will protect the Council from compensation claims provided the Direction takes effect not earlier than 12 months from the date of making.

4.0 Consultation

4.1 As the matter is a key decision and did not appear in the latest published Edition of the Forward Plan, the Chairman of the Scrutiny Committee was notified and that notification was placed on deposit at the Gateway for five clear days prior to the date of decision. The Article 4 Direction, once made, was placed on deposit for 28 days and was the subject of public notification.

5.0 Representation received

5.1 The consultation period has now ended and 7 representations have been received. 4

of those support the making of the Direction, and 3 of those including the National Landlords Association (NLA) raise the following issues of concern.

- The NLA states that the establishment of a small HMO does not represent a substantial change of use in terms of the burden imposed on local infrastructure.
- Trends in the UK housing demographics point to a greater need for shared housing HMOs in Margate.
- Changes to the Local Housing allowance which take effect this April will create even greater need for shared accommodation.
- Anti social behaviour can be tackled under other powers.
- The aims of the Council could be better achieved through an accreditation scheme.
- The proposed Article 4 Direction will be likely to erode the ability of landlords in Margate to react to changing circumstances and the needs of the community
- HMOs provide needed accommodation for students
- The Direction would prevent new HMOs from forming but would not result in the loss of the existing ones as frozen communities.
- There is a need for low cost housing in Thanet, including for students.
- If concern is about tenant behaviour there are other ways of dealing with this rather than to change planning laws

5.2 In deciding whether to confirm the Article 4 Direction, the Cabinet will need to take account of the issues raised through the representations. However, in deciding whether to confirm the Direction members should bear in mind that the effect of the Direction will not would not mean a blanket ban on HMO's, as it would remain open to an owner to apply for permission for an HMO.

5.3 Any such planning application received as a result of the Direction coming into force will attract no fee; and will be considered by the Council against its planning policies and having regard to any other material factors that relate to that application. The Council would be able to consider any issues relating to housing need as well as any impacts on the amenity of the neighbourhood and any relevant wider considerations; and to decide any planning application accordingly.

5.4 The representations regarding the existence of other powers to deal with antisocial behaviour and the existence of the voluntary accreditation scheme do not, in my opinion impact upon the justification for the making of the Direction, and therefore the Officer recommendation is that the Direction be confirmed

5.5 This Article 4 Direction if confirmed would come into force one year after it was made, with the consequence being that after that date the change of use of a dwellinghouse to and HMO for between 3-6 people will not be a permitted change and instead planning permission would be required.

6.0 Options

6.1 To confirm the Direction; or, not to confirm the Direction.

7.0 Corporate Implications

7.1 Financial

7.1.1 None.

7.2 Legal

7.2.1 None

7.3 Corporate

7.3.1 The Confirmation of the Article 4 Direction would contribute to the corporate objectives of facilitating the provision of good quality housing for the community

8.0 Recommendation

8.1 To confirm the Direction.

9.0 Decision Making Process

9.1 This decision whether to confirm the Direction is a Cabinet decision.

Contact Officer: Simon Thomas, Planning Manager-(ext 7752)

HOMES AND COMMUNITIES AGENCY BID FOR NEW AFFORDABLE HOMES

To:	**Cabinet Meeting – 23 June 2011**
Main Portfolio Area:	**Community Services – Strategic Housing**
By:	**Lauren Hemsley – Senior Strategic Housing Officer and Craig George – Housing Services Manager**
Classification:	**Unrestricted**
Ward:	**All wards**

Summary: **To endorse the bid to the Homes and Communities Agency (HCA) to build new affordable units on Housing Revenue Account land.**

For Decision

1.0 Introduction and Background

1.1 As part of the Homes and Communities Agency's Affordable Homes programme 2011-2015, Registered Providers and Local Authorities were asked to bid for funding for the whole of the comprehensive spending review period by the deadline of 3rd May 2011. The deadlines set by the HCA have been very tight and there was not enough time to take a report to Cabinet prior to the submission of the bid. The HCA has less funding available than previous years. There is approximately £4.5 billion available of which £2.3 billion is already committed, compared with £8.1 billion of funding which was available from 2008-2011. The target for the funding is to deliver 150,000 affordable homes.

1.2 The grant funding available equates to less funding per unit compared with the previous framework. A new affordable rent model has, therefore, been the main focus of affordable housing delivery under the new framework. The intention is that Registered Providers charge a higher rent to tenants and for the additional rent collected to be used to deliver more affordable housing. Affordable rent has been set at up to 80% of market rents including service charges. The difference in rents in Thanet, however, does not generate sufficient additional income to make it appealing to Registered Providers. The example below demonstrates the rental differences for a typical 2 bedroom house in Margate:

Example: 2 Bedroom house in Margate	**Rent collected per week**
Thanet District Council rent	£72.76
Registered Provider rent	£83.13
Market rent (Local Housing Allowance)	£109.62
Affordable Rent (80% of market rent)	£87.69

Difference between current Registered Provider rent and affordable rent = an additional £4.56 per week.

1.3 This additional income is minimal and does not generate enough income to build new affordable homes. Under the new framework Registered Providers have submitted bids to the HCA for considerably fewer affordable units than previous years. We have therefore taken the view that to ensure new affordable units are delivered, TDC needs to bid for funding to develop some of the HRA land.

1.4 There is a larger difference between the rents of Thanet District Council affordable housing stock and the new affordable rent levels, which could generate a more substantial additional income. We need to ensure as a local authority, however, that we are providing accommodation which is affordable to tenants. Local authority rents are gradually being increased under the local authority rent restructuring to meet the levels of registered providers rents by 2016, and it considered that to suddenly increase rents to affordable rent levels before this time is not in the interest of tenants. This will be looked at in more detail in the Tenancy Strategy local authorities are required to produce in 2012.

1.5 The Local Authority New Build Programme which has delivered 5 new units with HCA funding in the last financial year has been a success. This has tackled anti social behaviour at derelict garage sites and helped to regenerate small parcels of land with liability costs. The bid to the HCA consists of a new build programme including other similar old garage sites as well as some larger sites, some of which already have outline planning permission.

1.6 Other funding streams are available such as £200million for Empty Homes and funding for Homelessness change. We have expressed an interest in these funding streams as well through the bid and further details will be available from the HCA in the next couple of months.

1.7 The bids made by TDC and Registered Providers now form the basis of discussion with the HCA in accordance with the East Kent Local Investment Plan and replace the previous delivery plan system.

2.0 The Current Situation

2.1 The main focus of TDC's bid to the HCA is new build. Registered Providers are required to demonstrate they are putting in their own funding by converting social rents to affordable rents, selling assets and inputting land. We have some suitable HRA land which we can contribute and will not convert any rents to affordable rent at this stage.

2.2 There is a presumption that any new units granted funding will be at the new affordable rent levels. As part of the negotiation process following the submission of the bid, we will need to work closely with the HCA to ensure that rents are affordable to tenants.

2.3 The figures have been calculated on the assumption that the grant funding will be at 40%. On this basis we will need to spend £2,517,000 from the HRA account and will be requesting £1,678,000 from the HCA. We are not proposing to undertake any borrowing and will utilise existing balances.

2.4 We can expect to hear from the HCA whether our bid has been successful over the next few months. As we are a local authority we cannot enter into an agreement with the HCA before April 2012 until after the final HRA settlement is confirmed. The build programme is therefore proposed to commence in April 2012.

3.0 Options

3.1 To endorse the HCA bid and financial spend from the Housing Revenue Account.

3.2 To withdraw the bid proposals and refuse the HRA spend.

4.0 Corporate Implications

4.1 Financial and VAT

4.1.1 The total cost to the council from the HRA budget is proposed to be £2,517,000 (this does not include site acquisition costs for one of the sites). To be funded through HRA revenue reserve contributions.

4.1.2 The HCA have confirmed they will not enter into an agreement with a local authority before April 2012 and until the final HRA settlement is confirmed. So the offer and discussions with the HCA are flexible until this time. We are not proposing to commence the build programme until 2012-13 for this reason.

4.1.3 There is a further cost analysis available should this be required.

4.2 **Legal**

4.2.1 Legal advice has been sought and the legal department are looking into the details of the sites. At this stage as the bid is only provisional and still open to discussion there is still time to undertake further works to ensure there are no restrictions on the land which would prevent the proposed development.

4.3 **Corporate**

4.3.1 The bid does not commit the Council to the programme and is for the HCA to assess and negotiate affordable housing delivery in the district.

4.3.2 There is no risk in submitting the bid. If we do not submit a bid, however, there is a risk that the Registered Providers bids alone will not create the new affordable housing supply needed by the district. The bid is in accordance with the Housing corporate priorities to provide a balanced housing market in the district, ensure there is housing supply to meet local demand, create safe and secure homes and for the council to deliver quality service to its tenants.

4.4 **Equity and Equalities**

4.4.1 The creation of 30 new units will help to tackle antisocial behaviour and deprivation on derelict sites and create new affordable homes for residents on the housing register. This will promote community cohesion and will create a range of accommodation to meet the needs of residents.

4.4.2 In the opinion of the writer there are no equity and equality implications to this report.

5.0 Recommendation

5.1 That Cabinet endorse the bid to the HCA and the Housing Revenue Account spend in order to build 30 new affordable homes over the period 2012-2015.

6.0 Decision Making Process

6.1 This is a budget decision to go to Cabinet who will need to consider the spend from the HRA reserves in order to build new affordable homes.

Contact Officer:	Lauren Hemsley – Senior Strategic Housing Officer
Reporting to:	Madeline Homer – Community Services Manager

Background Papers

Title	**Details of where to access copy**
2011-2015 Affordable Homes Programme - Framework	*http://www.homesandcommunities.co.uk/affordable-homes.htm*

Corporate Consultation Undertaken

Finance	Nicola Walker - Finance Manager - HRA, Capital & External Funding
Legal	Harvey Patterson – Corporate & Regulatory Services Manager

DATA PROTECTION ACT (1998) – POLICY & PROCEDURES

To:	**Cabinet Meeting - 23 June 2011**
Portfolio Area:	**Regulatory Services**
By:	**Gary Cordes, Legal Services Manager**
Classification:	**Unrestricted**

Summary: **To consider and approve Policy & Procedures for a new Council-wide data protection strategy in accordance with the Data Protection Act 1998.**

For Decision

1.0 Introduction and Background - The Data Protection Act (1998) - What is it?

1.1 The DPA prevents organisations from using personal information for purposes an individual might lawfully object to. It does so by specifying how these organisations can use, store and share the personal data they collect. It also gives individuals the right to see any personal data held about them, and to have inaccurate information corrected. The Act calls anyone who holds personal data a 'data controller' and the individual whose personal data is held the 'data subject'. Sometimes the data controller will arrange for a third party 'data processor' to handle personal data on its behalf. In those circumstances (perhaps under shared service arrangements or through an ALMO) a data processor contract must be put in place to comply with the Act. Where data is shared, for example, with DWP for investigation purposes, appropriate data sharing protocols need to be in place.

The Act refers to the 'data protection principles' which are as follows:

- Processing must be fair and lawful
- Data will be obtained only for specified and lawful purposes
- The data process shall be adequate, relevant and not excessive
- It will be accurate and up-to-date
- It will be kept no longer than necessary
- Processing shall be in accordance with the rights of data subjects and
- Data will be held securely

These principles are key to ensuring that the council is fully compliant with the Act.

2.0 Council Inspection and Report

2.1 A Final Audit Report Assurance Statement dated August 2010 provided "limited assurance with regards to compliance to the requirements of the DPA 1998 generally….". Audit recommendations were made, as a result of which the Corporate and Regulatory Services Manager has been tasked with ensuring that the Council fully meets its obligations under the Act as soon as possible. The Legal Services Manager was appointed to project manage the implementation of the measures required to ensure full compliance with the Act, as outlined within the audit recommendations. The project is well under way and Cabinet approval and endorsement is now sought for the items detailed below to ensure that all staff and other users of personal data under Thanet District Council's control embrace the new policies and procedures and other listed requirements, so as to provide full compliance with the DPA and, in turn, to keep business risk to a minimum.

3.0 Cabinet endorsement is requested for the following:

3.1 Approval of the annexed draft policies, procedures and appendices (1-9)

3.2 Publication of Forms and Documents

3.2.1 Approval for the above forms and documents to be published on appropriate sections of TOM and/or the internet, for public use

3.2.2 Estimated completion date: July/August 2011

3.3 Appointment of a nominated Data Protection Officer for Thanet District Council

3.3.1 The Corporate and Regulatory Services Manager to be appointed as the Council's Data Protection Officer (DPO).

3.3.2 The Legal Services Manager to be appointed as the Council's Deputy DPO.

3.3.3 Approval for the DPO to be responsible officer for the annual DPA Notification.

3.4 Awareness & Training

3.4.1 Approval of a Council wide 'Data Protection Awareness Week' to be devised in conjunction with the Communications team (estimated date of completion: July/Aug 2011).

3.4.2 A requirement that all relevant managers ensure that staff who control/process personal data undertake the EKHR partnership's 'Ivysoft' data protection training module.

3.4.3 Such training to be organised by the DPO and completed within a timescale to be set by the DPO

3.4.4 Estimated completion date: July-Sept 2011

4.0 Service Compliance

4.1 Statement requiring all Tier 2 Managers and above to ensure all DPA policies, procedures, training (including induction training), individual service plans and risk registers are fully complied with/maintained up to date and embedded within their individual service areas,

4.2 Including the need to provide the Data Protection Officer with prompt responses to any questionnaire/checklist required to enable him to check that all service areas are properly complying with the DPA. These responses may include providing the DPO with copies of relevant forms, notices, and protocols/data sharing agreements, where relevant to individual service areas

4.3 Estimated date for circulation of questionnaire/checklist: July 2011;

4.4 For review of checklist: Sept 2011;

4.5 For management compliance with remainder of above requirements: December 2011

5.0 Corporate Implications

5.1 Financial

5.1.1 Approval for expenditure up to £1,750 for the hire of a specialist training consultant for 'higher level' DPA training to all Tier 1 and Tier 2 Managers and above with data control/processing responsibilities (estimated completion date: Sept 2011).

5.1.2 Approval for expenditure up to £1,100 for purchase of the Encyclopaedia of Data Protection & Privacy, plus annual update fees payable every September of c. £850.

5.1.3 Approval for payment of the council's annual registration ('Notification') fee by standing order or direct debit (reduces risk of failure to Notify with resultant fines/bad publicity).

5.2 Legal

5.2.1 Failure to comply with the Data Protection Act could result in the council being liable to fines of up to **£500,000**. Failure to comply with the DPA also risks claims from individuals seeking compensation for alleged breaches of the Act.

5.3 Corporate

5.3.1 Approval for inclusion in staff induction manual of section on DPA compliance and responsibilities of individual employees handling personal data in accordance with the Act.

5.3.2 Failure to adopt a robust DPA strategy could result in reputational and financial damage to the Council

5.4 Equity and Equalities

5.4.1 Training of all TDC staff handling personal data will be provided. Both staff and the public will be provided with full details of TDC's commitment to protecting individuals' personal data, and to allowing appropriate access to such data, primarily via TOM and the Council's internet site. There will be ongoing consideration of the impact of DPA policies and procedures and these will be amended if/when it is found necessary so as to ensure full ongoing compliance with our equality obligations.

6.0 Recommendations

6.1 That Cabinet approves the DPA Policy and Procedures Guidance Note

6.2 That the draft DPA Policy and Procedures Guidance Note be submitted to the Cabinet for final approval

6.3 That the draft DPA Policy and Procedures Guidance Note be published on the internet and intranet pages

6.4 The Corporate and Regulatory Services Manager to be appointed as the Council's Data Protection Officer (DPO).

6.5 The Legal Services Manager to be appointed Deputy DPO.

6.6 That expenditure of up to £1,750 for the hire of a specialist training consultant for "higher level" DPA training to Managers with data control/processing responsibilities (estimated completion date: September 2011) be approved, and that funding be provided by means of a priority draw on the training budget.

6.7 That expenditure of up to £1,100 for the purchase of the Encyclopaedia of Data Protection & Privacy, plus annual update fees payable every September of c. £850 be approved, subject to virement funding within the Corporate & Regulatory Services' budget;

6.8 That payment of the Council's annual registration ('Notification") fee by standing order or direct order or direct debit be approved;

6.9 That Cabinet supports a council-wide officer training programme, subject to the findings of the questionnaire referred to in the report and a pragmatic approach being adopted.

6.10 That Cabinet supports a Data Protection Awareness Week.

7.0 Decision Making Process

7.1 This is a Policy framework document for SMT and then Cabinet approval.

Contact Officer:	Gary Cordes, Legal Services Manager
Reporting to:	Harvey Patterson, Corporate & Regulatory Services Manager

Background Information

Title	Where to Access Information
	www.ico.gov.uk

Annex List

Annex 1	DPA Policy for Officers and Members and appendices (1-9)
Annex 2	Subject Access Request Form
Annex 3	Data Security Breach Policy
Annex 4	Notes on Data Protection Act
Annex 5	Flowchart
Annex 6	Checklist Final Data Protection
Annex 7	Data Protection External Page
Annex 8	How we use your information
Annex 9	Privacy Statement for webpage

Corporate Consultation Undertaken

Finance	N/A
Legal	Harvey Patterson, Corporate & Regulatory Services Manager

THANET DISTRICT COUNCIL

DATA PROTECTION ACT 1998

POLICY & PROCEDURES

Version Control

Version 1 – 13 April 2011
Version 2 – 21 April 2011
Version 3 - 4 May 2011

Gary Cordes
Legal Services Manager
Corporate & Regulatory Services
Thanet District Council
PO Box 9
Cecil Street
Margate CT9 1XZ

Contents

1. SUMMARY

Thanet District Council must ensure all personal information is processed in accordance with the Data Protection Act 1998. The policy explains how Members and Officers are expected to comply with Act. The Council must comply with this policy to the ensure Data Protection Act is not breached. Any breach of the Act has serious consequences for the organisation and its customers.

2. INTRODUCTION

The Data Protection Act 1998 (The Act) aims to protect all personal data which is collected, processed, stored and disposed of by an organisation. Personal data is information about a living, identifiable person. The Act applies to data in paper and electronic format.

The Act supports Article 8 of the Human Rights Act, which gives an individual 'the right to respect for his private and family life, his home and his correspondence.'

Everyone must respect confidentiality in the working environment. We must take care in disclosing information to others – within our own teams and sections, to other services within the Council and externally to other organisations.

The Information Commissioner's office (ICO) is responsible for regulating and enforcing the Act. The ICO is an independent authority which has legal powers to ensure organisations comply with the Act. Fines of up to £500,000 can be issued to organisations which breach Data Protection requirements.

3. SCOPE

This policy applies to elected members and all employees working for the Council, (including consultants, volunteers and contractors) and external data processors instructed by the Council who are handling data on behalf of the Council. Everyone handling personal data should understand and comply with the principles of the Data Protection Act.

4. POLICY STATEMENT

It is the responsibility of all Tier 2 Managers to ensure that their staff are aware of and adhere to this and all other Data Protection Act (DPA) policies and procedures and have received relevant Ivysoft training. Tier 2 Managers must ensure that all new staff complete the latest induction training that includes a section on DPA. All new DPA requests, data breaches or suspected data breaches must be referred immediately to the Deputy Data Protection Officer in Legal Services. Tier 2 Managers shall arrange the destruction of personal data as soon as possible after minimum retention periods have expired. Contact the Deputy Data Protection Officer in Legal Services if you are uncertain about any aspect of the Council's DPA policies and procedures or the DPA generally.

The Council is committed to ensuring compliance with the Act and will:

- Respect the rights of each individual
- Be open and honest about the personal data it holds

- Provide training and support to those handling personal data in the course of their duties
- Notify the ICO that it processes personal data. This is a statutory requirement and notification must be submitted annually. Notification must be kept up to date. Any changes to the use of personal data being updated within 28 days. The Democratic Services Manager maintains the annual notification with the ICO on behalf of the DPO.
- Inform the ICO of breaches of the Act (where required)

5. WHAT IS PERSONAL DATA?

Any personal information that is processed, is readily accessible and relates either directly or indirectly to a living, identifiable person who can be identified from the data or from data and other information which is in the possession of, or is likely to come into the possession of the Data Controller.

Personal data includes an expression of opinion about the individual and any indication of the intentions of the Data Controller, or any other person in respect of the individual.

6. OTHER DEFINITIONS

Data Controller — All users of personal information are Data Controllers (individuals and the Council as a whole).

Data Protection Officer — The responsible person within the Council for all matters connected with the Data Protection Act. The Data Protection Officer is also responsible for notifying the Information Commissioner of personal data held and processed by Thanet District Council.

Data Subject — The individual to whom the information relates.

Disclosure Recipient — Organisations or individuals to whom the data can be given or disclosed.

Personal Data: — Data relating to a living individual who can be identified from that data (or from that data combined with other information in the possession of the Data Controller).

Processing — Obtaining, recording, holding or carrying out any set of operations on the information or data, including organising, adapting, altering, retrieving, consulting, using, transmitting, disseminating, making available, aligning, combining, blocking, erasing or destroying.

Sensitive Personal Data: — The Act makes a distinction between ***Personal Data*** and ***Sensitive Personal Data.*** Sensitive Personal Data includes:

- Racial or Ethnic Origin
- Political Opinions or Persuasion
- Trade Union Membership or Affiliation
- Physical or Mental Health or Condition
- Sexual Life
- Commissioned or Alleged Commission of Offences

- Any proceedings for any offence, committed or alleged, including any sentencing decisions made by the Court.

Subject Access Anyone who thinks that the Council is holding data about him or her is entitled to receive a copy of the information or to be told that no data is held about them. Applicants must identify themselves and specify which data they wish to see. Applications should in the first instance be made in writing to the Data Protection Officer. The Council is under a legal obligation to comply with a subject access request (SAR) submitted with the required fee (currently £10) within 40 days of its receipt.

Source Where the data entered into a computer system or filing system originates from.

7. THE RIGHTS OF THE DATA SUBJECT

The Act provides individuals with a number of rights relating to their personal data:

7.1 **Accessing Information:** This allows an individual to find out what personal data the Council holds about them. For further information please refer to the Subject Access Request (SARS) Policy & Procedures (Annex 1)

7.2 **Correcting Information:** An individual has the right to correct, block, remove or destroy personal details which are factually inaccurate. This may be agreed with the Council's Data Controller. In some cases the Data Subject may need to refer to the ICO, or apply for a court order to make these changes. In all cases the Council must keep the original data as a record of its actions, even is this has been corrected. A copy of the amended record should be sent to the Data Subject for their records.

7.3 **Preventing Processing of Information:** The Council can be asked not to process data which may cause substantial or unwarranted damage or distress to the individual. The Council is not always bound to act on the request.

7.4 **Preventing Unsolicited Marketing:** The Council is required not to process data about an individual for direct marketing purposes, when the individual has specified he/she does not want direct marketing, e.g. sending unsolicited mail.

7.5 **Preventing Automated Decision Making:** An individual can object to decisions being made by automatic means, i.e. where there is no human involvement.

7.6 **Claiming Compensation:** An individual can claim compensation from the Council through the courts for damage and, in some cases, distress, caused by any breach of the Act.

7.7 **Requesting a Review of Data Processing:** An individual can ask the ICO to investigate and assess whether the Council has breached the Act.

8. THE 8 DATA PROTECTION PRINCIPLES

The Act states that anyone who processes personal data must comply with 8 principles which ensure that personal information is:

8.1 Fairly and lawfully processed

8.2 Processed for limited purposes

8.3 Adequate, relevant and not excessive

8.4 Accurate and up to date

8.5 Not kept for longer than is necessary

8.6 Processed in line with your rights

8.7 Secure

8.8 Not transferred to countries outside the European Economic Area (EEA) without adequate protection.

9. ROLES AND RESPONSIBILITIES

Thanet District Council has appointed the Corporate and Regulatory Services Manager as the Data Protection Officer with responsibility for ensuring all members of staff handling personal data are compliant with the Act. The Legal Services Manager will be Deputy Data Protection Officer.

Anyone representing the Council has a duty to protect the information it holds. Access to personal data must be on a strict need to know basis. Personal data must not be discussed or disclosed without appropriate authorisation.

Any member of staff who knowingly or recklessly breaches the Council's Data Protection Policy and Procedures may be subject to internal disciplinary procedure. This is in addition to the civil and criminal remedies available to the Information Commissioner under the Act.

.Authorisation from a Tier 2 Manager must be obtained before an employee is permitted to use a privately owned computer to process personal data belonging to the Council or to take personal data out of the Council's offices for processing on a computer owned by the Council or for any other purpose.

10. ELECTED MEMBERS

Elected members may have access to, and process personal data, in the same way as employees, and must comply with the 8 Data Protection Principles. Since data held on council systems may be used by elected members in their other roles the data controller may be the elected member or the council individually, jointly or on behalf of others.

Notification should be arranged as follows:

- When acting on behalf of the council, councillors can rely on the Council's notification.
- When acting on their own behalf (e.g. when dealing with complaints made my local residents) councillors must notify the ICO in their own right.
- When campaigning within their own political party councillors may rely on the notification made by their party.

For ease of retrieval elected members should store council data separately from data relating to their other work (e.g. ward and political party work).

11. PRIVACY NOTICE (FORMERLY FAIR PROCESSING)

All Thanet District Council forms and notices which expect an individual (data subject) to provide personal information require a mandatory privacy notice. For this purpose, managers must ensure that a suitably worded 'privacy notice' is attached to all forms on which personal data is being collected. The privacy notice will explain why the information is being collected and, where relevant, set out how and why the information will be shared within the Council.

Data collected for a specific purpose e.g. council tax, cannot be used or disclosed for any other purpose without the permission of the data subject.

A privacy notice should state the following:

1. the name of the service e.g. Commercial Services
2. The purpose(s) for which the data is to be processed
3. Point to where more detailed information can be found e.g. weblink

12. SUBJECT ACCESS REQUESTS (SARS)

Individuals have a right to access information about themselves. Thanet District Council will disclose any information it holds (applying any appropriate exemptions) within 40 calender days of receiving a request and acceptable identification.

The Council will charge the current maximum £10 fee allowed for processing data access requests.

Every request for access, whether from the Council's own employees or the public, should be directed to the Data Protection Officer who will respond to all requests.

The SAR request form (with notes on completion) is attached at Annex 1

13. PERSONAL DATA HELD BY THANET DISTRICT COUNCIL

The Council's notification is available for inspection on the Information Commissioner's website: www.dpr.gov.uk/search.html.

The Council's number for accessing its entry is Z5398859.

Please note that for the purposes of this policy, 'data' includes all information including that held on physical files.

Personal data will be kept in an appropriately controlled and secure environment both within Council premises and if any such data is removed from Council premises.

14. TRAINING

Tier 2 Managers are responsible for ensuring that Thanet District Council's Data Protection Policy is communicated and implemented within their area of responsibility with appropriate levels of supervision.

All new and existing staff will undertake the "Ivysoft" training module on data protection and familiarise themselves with the DPA pages on TOM which will include guidance in the form of flowcharts, FAQs, and links to the relevant forms including our DPA Policy and Procedures. More in depth training will be provided to Tier 1 & 2 Managers and for other staff working in specialist roles.

A Managers Toolkit will be provided online as part of the 'Officers Handbook' due for publication in July 2011 which will also form part of the induction of new members of staff.

Each employee has an individual responsibility to be aware of their statutory responsibility for following good data protection practice.

15. BREACHES OF THE ACT

A breach of the Act may arise from a theft, accidental loss by an employee, a deliberate attack on the Council's systems, unauthorised use of personal data by an employee or equipment failure.

In the event of a breach staff should follow the Data Security Breach Policy (attached at Annex 2).

16. INFORMATION SHARING

Data sharing and/or processing with external agencies (including shared services arrangements and ALMO's) will be the subject of a written data protection agreement setting out the powers that permit the sharing/processing, its scope and controls and will be subject to approval by the Data Protection Officer prior to sign-off. If you are sharing data and the sharing is not clearly part of your routine statutory function, you must ensure that an appropriate agreement is in place. Contact the Data Protection Officer for further details and advice.

17. PRACTICAL GUIDANCE FOR MEMBERS AND OFFICERS FAQs

What does the Act mean for employees?

The Council is committed to compliance with the Act. Managers should ensure that their area of operation complies with the Act, that their use of personal data is registered (via the Data Protection Officer) and that staff are aware of the policy and procedures to be followed. This includes ensuring that all new and existing staff undertake the "Ivysoft" training module on data protection, have read and understood this policy document and are familiar with the Data Protection Act page on TOM. Each employee has an individual responsibility to be aware of what the Act involves and how to comply with it.

What does the Act mean for Members?
Elected Members should make themselves aware of and comply with this policy when engaged on Council work. Members must ensure that their use of personal data in their constituency work is registered with the Information Commissioner. There should be a clear separation between the data held for Council work and that held for constituency work.

How do I know if I can disclose personal data for a particular purpose?
Generally, data held by the Council is not to be disclosed outside the Council unless required by law. Disclosures within the Council are permitted if they are necessary for an officer to carry out their normal duty but the purpose must be compatible with the purpose for which it was originally gathered. There will be occasions when confidentiality will not allow even internal disclosure. Contact the Data Protection Officer for further information if you are at all uncertain about any specific situation.

How do I deal with requests from external organisations to share data?
All requests, whether from individuals or external agencies including for example the police, DWP or a Health Authority, should be passed immediately to the Data Protection Officer who will advise whether or not the request may be complied with. If any agency proposes a long-term partnership in data sharing, a written agreement must be prepared, stating what powers it has to enter into such an agreement, who will manage the exercise and what controls will be in place to protect the information. All such agreements must be approved and signed-off by the Data Protection Officer, who shall retain the original versions of such agreements on behalf of the Council. For detailed advice contact the Data Protection Officer. It should be noted that, if a request is made regarding an individual, the agency making the request should specify, in writing, why it requires the information, and the legal authority for requesting such information.

What about publicly available information?
When you receive a request, first check the Council's publication scheme to see if the information is already in the public domain. If you think this is the case, please advise the Data Protection Officer when sending the request to him.

What personal data does the Council hold?
The Council's notification is available for inspection on the Information Commissioner's website: www.dpr.gov.uk/search.html. The Council's number for accessing its entry is Z5398859.

What about manual/physical files?
Manual files are covered by the Act. Subject access to manual files is permitted and any processing that involves manual files must be notified to the Information Commissioner.

Can we carry out 'Data Matching'?
Data matching is the act of examining data held in two or more systems in order to check whether there is any recorded information common to both or all of those systems that indicates that the information relates to one and the same person. The Council may carry out data matching if there is a clear justification for it, such as the detection of fraud.

Does the Council disclose to the Police/DWP/Other Agencies?
Local Councils may disclose to other agencies for the purposes of the "prevention of crime or apprehension of offenders", anti-social behaviour and community safety as

permitted under Section 115 of the Crime and Disorder Act 1998. There is no general disclosure to external agencies. Again, all requests must be sent to the Data Protection Officer for processing/formal response.

Where may I obtain further information and advice?

1. See TOM – "The Data Protection Act"
2. Visit: www.ico.gov.uk/for_organisations/sector_guides/local_authority.aspx
3. If you require further assistance, please contact the Data Protection Officer, Harvey Patterson or his delegate, Gary Cordes in Legal Services.

Appendices

Appendix 1 Sars Form **+ notes**

Appendix 2 Breach Policy **+ Form**

Appendix 3 TOM Page

Appendix 4 Flowchart**: Managers Guide to Sharing Information**

Appendix 5 Checklist

Appendix 6 TDC Internet Page

Appendix 7 **Information Booklet for Customers**

Appendix 8 Privacy Statement

This page is intentionally left blank

THANET DISTRICT COUNCIL

SUBJECT ACCESS REQUEST FORM

Data Protection Act 1998 – Subject Access Request.

Please provide the following details about yourself:

Full Name: ……

Address: ……

……

……

Telephone No: …….. Fax No: ……..

Email: ……..

Fee: A payment of £10 (the current statutory maximum) is payable for each application for information. Please enclose a cheque or postal order made payable to Thanet District Council. Your request will be processed within 40 days of receipt of a fully completed form. If the information contains details of another person we may need to seek their consent or redact (remove) that information before we can provide the information to you.

1. Are you requesting information about yourself?

If so, you are the Data Subject and documentary evidence of your identity is required, i.e. driving licence, birth certificate (or photocopy) and stamped addressed envelope for returning the document. Please go to Question 3 below.

If you are not the Data Subject, please supply the written consent of the Data Subject and supply their details as follows:

Full Name: ……

Address: ……

……

……

Telephone No: …….. Fax No: ……..

2. Please describe your relationship with the Data Subject and briefly explain why you are requesting the information on their behalf.

……

……

……

3. Please describe the information you seek, together with any names and/or dates you may have which may help us identify the information you require.

……..

……..

……..

4. Declaration

I …… confirm that the information given on this application form to Thanet District Council is true. I understand that Thanet District Council may need more information to confirm my identity/or that of the Data Subject to locate the information I am requesting.

Signature: …….. Date: ……

5. Documents to return with the completed form:

a. Evidence of your identity

b. Evidence of the Data Subject's identity (if different from above)

c. Evidence of the Data Subject's consent to disclose to a third party (if relevant)

d. A fee of £10 (cheques to be made payable to Thanet District Council)

e Stamped addressed envelope for return of Proof of Identity/authority document.

Please note: the Council reserves the right to redact (remove) information that relates to other third parties (under the provisions of Section 7 of the Data Protection Act 1998).

6. Please return the completed form to:

The Data Protection Officef
Thanet District Council
PO BOX 9
Cecil Street
Margate
CT9 1XZ

7. Office Use Only

Date request received: …….

Date completed: …….

Notes: …….

……

NOTES ON COMPLETION OF SUBJECT ACCESS REQUEST FORM

Please read these notes carefully before completing the details on the Subject Access Request Form.

1. Who may apply for information? Only the individual who the personal information is about (*the Data Subject*). This means that you can only apply for your own personal information (*referred to as Subject Access Request*). You cannot apply for information about anyone else; neither can anyone else apply for information about you. You may wish to nominate someone to be your authorised representative and the information can then be released to them but only after your consent has been given.

2. What does it cost? The Council charges the prescribed fee of £10 for processing requests for access to personal data, which we are entitled to do under the provisions of the Data Protection Act 1998. Please include a cheque made payable to Thanet District Council with your Application Form.

3. How soon do I get an answer? Within 40 calendar days of the Council receiving your written request, the fee and proof of identity. Please bear in mind that the Council has many different departments, therefore, it is important to be as specific as possible when requesting your personal information. If we do not have enough information to begin our search, we will write to you and ask you for more details. In these circumstances the 40 days response time will begin from the day the Council receives sufficient information from you to proceed.

4. Identification. The Council must not knowingly give personal information to the wrong person and we must do our best to ensure that the personal information we have been asked for is given only to the person to whom this information refers, or their authorised representative. Therefore, we will be asking you for proof of both your identity and address.

5. Children. Children have the same rights of access to their own personal information as adults and the same rights of privacy. There is no minimum age but current guidance from the Information Commissioner's Office identifies that as a general guide, a child of 12 or older is expected to be mature enough to understand the request they are making. When a subject access request is received from a child, the Council will assess whether the child has the capacity to understand the implication of their request and of the information provided as a result of that request. If the child does understand, then their request will be dealt with in the same way as that of an adult. If a parent or legal guardian makes a request on behalf of a child, the request will only be complied with when we have received assurances that the child has authorised the request and that their consent was not obtained under duress or on the basis of misleading information. If the child does not understand, then a request from a parent or legal guardian for the child's information will only be complied with when assurances are received that they are acting in the best interests of the child.

6. Please complete and return the Subject Access Request Form to the address below, together with the £10 fee, proof of identity (e.g. copy of passport or photo driving licence), proof of address (e.g. copy of utility bill or address section of bank statement) and if you are applying on someone's behalf, proof that they have given consent.

The Subject Access Request Form should be sent to:

Data Protection Officer
Thanet District Council
PO Box 9
Cecil Street
Margate, CT9 1XZ

This page is intentionally left blank

THANET DISTRICT COUNCIL

DATA SECURITY BREACH POLICY

MARCH 2011

1.1 Policy Statement

Thanet District Council holds large amounts of personal and sensitive data. Great care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is crucial that prompt action is taken to minimise any associated risk to both the individual and the Council as soon as possible. This policy sets out the standards by which the Council will respond to a breach or unauthorised disclosure of Council-held data.

1.2 Scope

This policy applies to all TDC employees, Contractors, Councillors and anyone else with access to personal and/or sensitive data held by the Council.

1.3 Legal Context

The Data Protection Act 1998 provides for the regulation of processing (or use) of information relating to individuals, including the obtaining, storage, use or disclosure of such information.

Principle 7 of the Data Protection Act 1998 states that organisations which process personal data must take "appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

1.4 Types of Breach

Recent developments: in 2010 the Information Commissioner's Office (ICO) imposed its first fine of £100,000 against a Council that sent by fax personal information to the wrong recipient. In February 2011 Gwent Police signed an undertaking with the ICO after emailing the results of 10,000 Criminal Records Bureau checks to the wrong email recipient. It took the press of one button to get it so badly wrong! Take particular care when using fax/email to send personal data and always check you are using correct fax numbers/email addresses before transmitting data. ***For specific guidance on this area go to:***

http://www.ico.gov.uk/for_organisations/data_protection/security_measures.aspx

A data security breach can occur for a number of reasons:

- Loss, theft or inappropriate transmission of data, or loss/theft of equipment on which data is stored. This will include processing machines such as PC's, laptop computers, mobile telephones and faxes, as well as portable media such as memory sticks and discs. Where possible, data should be encrypted – contact IT for further advice.

- Inadequate access controls in systems, both manual and electronic, allowing unauthorised use, including unauthorised access to Council premises where data is held.
- Equipment failure.
- Human error.
- Unforeseen circumstances such as fire or flood.
- Unauthorised access through hacking.
- Information obtained by deceit, known as 'blagging'.

1.5 Containment and Recovery

Data security breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from specialists across the Council such as IT, HR, Communications and Legal Services and in some cases, contact with external stakeholders and suppliers. In cases of data theft, the police may be informed.

The person who discovers/receives a report of a breach must inform the relevant Tier 2 Manager, who must notify the Data Protection Officer as soon as they become aware of the beach. If the breach occurs or is discovered outside normal working hours, this should begin as soon as practicable. The Tier 1 manager must always be notified of any breaches.

If the breach involves a Tier 1 Manager, he/she must inform the Data Protection Officer direct.

The relevant Manager and Data Protection Officer must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effects of the breach. An example might be to shut down a system or to alert relevant staff.

The Tier 1 Manager and DPO must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

The relevant Tier 2 Manager, with input from the DPO where required, must quickly take appropriate steps to recover any losses and limit damage. Steps might include:

- Attempting to recover lost equipment.
- Contacting Revenues and Benefits or other relevant Council Departments, so that they are prepared for any potentially inappropriate enquiries (phishing) for further information on the individual(s) concerned. Consideration should be given to a global email across the Council. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details and confirm that they will ring back the person making the enquiry. Whatever the outcome of the call, it should be reported to Tier 2 Manager and DPO immediately.

- Contacting the Communications Team so that they can be prepared to handle any press enquiries.
- The use of back-ups to restore lost/damaged/stolen data.
- If bank details have been lost/stolen, consider contacting banks direct for advice on preventing fraudulent use.
- If data breaches involve use of entry codes or passwords, these codes must be changed immediately, and the relevant agencies and members of staff informed.

The relevant Tier 2 Manager will action the following:

- Complete a Data Protection Security Breach Notification Form.
  (also attached at the end of this document)
- Promptly submit the form, together with any additional details of the breach and actions taken, to the DPO.

1.6 Investigation

- The DPO will immediately action a Data Protection Security Investigation, to include all facts from the start of the breach to completion and sign-off of the matter. The Investigation will result in a detailed written record that explains the facts of the case and what steps have been taken to minimise the effects of the breach and to prevent similar further breaches including, where necessary, recommendations for procedural and system changes and staff training. The following should be taken into consideration as part of any investigation:

- What type of data is involved?

  Does the data relate to individual, living persons or is it non-personal?

- How sensitive is the data?

  Some data will be sensitive because of its very personal nature, for example health records, while other data types are sensitive because of what could happen if misused eg bank account details.

- What security was in place if any?

  For example, if data has been lost or stolen, were there any protections in place to protect the data, such as restricted room access controls operating correctly, or encryption and password protection for electronic data removed from the office? Or what procedures exist to prevent data being transmitted erroneously to wrong recipients via fax, email or by post?

- What has happened to the data?
  If data has been lost or stolen it poses a different risk than that applying if the data is corrupted or damaged.

- Can the data be restored or recreated?
  Assess if the situation can be eased by recovery or partial recovery of lost or corrupted data.

- How useable is the lost data?
  Assess what would happen should the data get into wrong hands. Is the data particularly sensitive or is it largely meaningless to the general public?

- How many individuals' personal data are affected by the breach?
  Whilst any breach is serious, clearly more damage is likely to occur if a large amount of data is involved.

- Whose data has been lost?
  Who are the individuals whose data has been breached? Whether they are staff, customers, clients, suppliers or other individuals will to some extent determine the level of risk posed by the breach and, therefore, any actions in attempting to mitigate those risks.

- What harm is likely to come to those individuals?
  Are there risks to personal physical safety or reputation, of financial loss or a combination of these?

- What other considerations are there?
  Consider the possible wider consequences of the breach and what steps may be taken to mitigate these, such as loss of public confidence in an important service we provide.

- Can the data be used for fraudulent purposes?
  Can the data be used for ID fraud? If individuals' bank details have been lost, consider contacting the banks themselves for advice on how they can help to prevent fraudulent use.

1.7 **Notification of Breach**

see ICO guidance note at:
http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/breach_reporting.pdf

Notification to individuals whose data has been breached should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

Decision to Notify

Answering the following questions will assist in deciding whether to notify:

1. **Will revealing the breach further compromise security?**
   Can notification help or hinder meeting security obligations with regard to the Seventh Data Principle which requires the Council to keep data secure?

2. **Can notification of the breach help the individual?**
   Bearing in mind the potential effects of the breach, could individuals act on the information provided to mitigate risks to them, for example by cancelling a credit card or changing a password?

3. **How many individuals are affected?**

If more than one thousand people are affected by the breach, or there are likely to be very serious consequences, the ICO will be informed in accordance with paragraph 2.1 below.

4. **Can the people affected by the breach understand the issue?**
   Consider how notification can be made appropriate according to the individual(s) concerned, for example if notifying children or vulnerable adults.

5. **Is the breach relatively minor?**
   Not every incident will warrant notification and notifying all customers when the beach affects a small percentage may well cause disproportionate enquiries and additional work.

6. **How are the details communicated?**
   Consideration should be given to who should be notified, what the message is, how it will be communicated and the security of the communication medium used.

7. **Who else needs to know?**
   Ensure the appropriate regulatory body is notified. A sector specific regulator may require TDC to notify them of any type of breach. Remember - the ICO should only be notified where a breach involves personal data.

   Tier 2 Managers must ensure their Tier 1 Manager is fully appraised and consulted concerning any breach notification.

1.8 Data Breach Notification Requirements

1.8.1 A description of how and when the breach occurred and what data was involved.

1.8.2 Include details of what steps have already been taken to respond to the risks posed by the breach.

1.8.3 Give specific and clear advice on the steps those affected can take to protect themselves and also what you are willing to do to help them.

1.8.4 Provide a contact point for further information or to ask you questions about what has occurred.

1.8.5 Record what happened in writing.

1.9 Evaluation and Response

Once the initial aftermath of the breach is over, the relevant Tier 1 Manager should fully review both the causes of the breach and the effectiveness of the response to it. The DPO and any other relevant Officer should be updated and a report should then be made by the DPO for submission to the next available SMT meeting, including recommendations for changes to this and any other DPA policy and/or procedure necessary to avoid repetition of the breach.

If systemic or ongoing problems are identified, then an action plan must be drawn up to remedy these problems. If the breach warrants a disciplinary investigation,

the relevant Tier 1 Manager leading the investigation should liaise with HR for advice and guidance.

This policy may also need to be reviewed following legislative changes, new case law or new/revised guidance from the ICO.

To reduce the risk of further breaches the following should be considered:

1. Identify what personal data is held and where and how it is stored.
2. Establish where the greatest risks are – usually determined by the sensitivity of the data.
3. Remedy any identified risk within the existing security measures.
4. Ensure when processing data, that the method of transmission is secure, always ensuring that only the necessary minimum amount of data is handled.
5. Address staff awareness of security issue via training and/or tailored advice.

2.0 Register of Hardcopy Data taken out of the Council Office

Managers shall establish and maintain a register of data taken out of the office to enable the recording and creation of an audit trail of hardcopy data which contains any or all of the following:

Personal data, sensitive personal data, restricted data and confidential information.

Before an officer takes any hardcopy data out of the Council offices, solely for the purpose of legitimate working requirements, they must undertake a proper assessment of the hardcopy data to establish if it contains any of the data outlined above. If after assessment the hardcopy data does contain such data, the officer must record the details of the hardcopy data in the relevant Register held in their section for this purpose. Where appropriate, data should be encrypted prior to removal from the office to reduce the risk of any security breach.

The Register should include the following:

1. Description of the hardcopy data sufficient to identify it, ie file reference number, relevant dates.
2. The date the hardcopy data is taken out of the Council offices.
3. The name of the officer responsible for taking the hardcopy data out of the Council offices.
4. The reason for taking the hardcopy data out of the Council offices.
5. The date the hardcopy data is returned to the Council offices by the officer responsible.
6. The entries in the Register to be sequentially numbered.

Tier 2 Managers must ensure that all their staff are aware of and comply with the above procedure, along with all other DPA policies, procedures and training requirements.

Managers should conduct a monthly audit of the Register and report any breach to the DPO for remedial action to be taken.

2.1 Notification of Data Security Breach to Information Commissioner's Office.

Reference: Go to: www.ico.gov.uk, then search "data security breach" for ICO guidelines on this topic.

Although currently there is no legal obligation on data controllers to report breaches of security which result in loss, release or corruption of personal data, the Information Commissioner believes serious breaches should be brought to his attention. 'Serious breaches' are not defined, but the DPO will be responsible for making any such referrals, taking into consideration current ICO guidance along with the facts of the breach.

2.2 Implementation

This policy takes effect immediately. All Tier 2 Managers must ensure that staff are aware of and adhere to this and all other DPA policies and procedures and receive relevant Ivysoft training. Managers must also ensure that new staff are inducted using latest induction training materials that contain a section on DPA and that all new DPA requests are immediately referred to the DPO. Tier 2 Managers shall be responsible for ensuring DPA compliance for their Service at all times.

DEFINITIONS

Blagging	Persuade or deceive in order to get something for free
Confidential Information	Information the disclosure of which would give rise to an actionable breach of confidence. A breach of confidence will become actionable if: • the information has the necessary quality of confidence • the information was given in circumstances under an obligation of confidence and • there was an unauthorised use of the information to the detriment of the confider
DPO (Data Protection Officer)	• Data Protection Officer. Corporate and Regulatory Services Manager to act as the Data Protection Officer for the

	Council. Legal Services Manager to act as Deputy DPO • Handles all Subject Access Requests and investigates all breaches under the DPA; • Ensures the Council makes and pays for annual Notification to the ICO; • Keeps original versions of all data sharing contracts/protocols entered into by various Council Services in strong room. • Reviews the Council's DPA policies and procedures regularly to ensure ongoing compliance with DPA at strategic level. • Keeps staff up to date with latest developments in data protection law and practice.
Data Security Breach	Loss, theft, corruption, inappropriate access or sharing of personal or sensitive personal data.
Phishing	The act of tricking someone into giving out confidential information
Relevant Tier 1 Manager	Tier 1 Manager responsible for the service area in which the breach occurred
Restricted Data	Sensitive information about a significant number of identifiable living individuals. Information that could lead to significant financial/reputational damage to the Council, Partners/Suppliers or the Government
Sensitive Personal Data (as defined by the Data Protection Act 1998).	Personal Data consisting of: • Racial or ethnic origin • Political opinions • Religious or similar beliefs • Trade Union membership • Physical or mental health or condition • Sexual Life • Commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any Court in such proceedings.

THANET DISTRICT COUNCIL

Data Security Breach Notification Form

Complete as soon as possible after identifying an actual/potential breach and submit this form to the Data Protection Officer

What service area do you work in?	
When did the breach occur?	
Describe how the event took place	
In cases of stolen data, please provide crime reference report number	
What security measures were in place?	
What has happened to the data?	
Whose data was lost?	
What steps have been taken to contain the breach?	
Any other information you consider should be taken into consideration in respect of the breach/potential breach?	

Signed …… Date ……

Position ……

This page is intentionally left blank

The Data Protection Act

What is the Data Protection Act (1998)?

The Data Protection Act (DPA) prevents organisations, including commercial ones, from using personal information for purposes an individual might object to. It does so by specifying how these organisations can use, store and share the personal data they collect. It also gives individuals the right to see any personal data held about them.

What is personal data?

Anything that identifies a living individual e.g. name, address, date of birth, some e-mail addresses, information about religious or similar beliefs. The Act calls anyone who holds personal data a 'data controller'. Any individual whose personal data is held is called a 'data subject'.

Using the Data Protection Act

Under the DPA, all personal information held by the Council must comply with the statutory data protection principles. This means when using personal data:

- processing must be fair and lawful
- it will be obtained only for specified and lawful purposes
- the data processed shall be adequate, relevant and not excessive
- it will be accurate and up-to-date
- it will be kept no longer than necessary
- processing shall be in accordance with the rights of data subjects.
- it will be held securely

An individual has the right to:

- ask the Council if it holds personal information about them
- be given a description or copy of the information with any unintelligible terms explained.
- be given details about purposes for which the Council uses information and other organisations to which it is disclosed
- ask for incorrect data to be corrected
- ask the Council not to use personal information about them for direct marketing
- to be given any information available to the Council about the source of data.
- to be given an explanation as to how any automated decisions taken about the data subject have been made.

If you collect personal data you must understand that the following must be treated as sensitive personal data and be processed fairly and lawfully, avoiding damage or distress to the subject of the data:

- Racial or ethnic origin of the data subject
- Political opinions of the data subject
- Religious beliefs or other beliefs of a similar nature
- Membership of a trade union
- Physical or mental health or condition of the data subject
- Sexual life of the data subject

What must I do if I receive a request for personal data?

1. Where possible the Subject Access Request Form should be completed. These are available via the TDC website.

2. If you cannot issue the Subject Access Request Form, then advise the data subjects that they must provide the following information prior to the request being processed:

   - They need to apply in writing
   - They need to specify what data they would like to see

3. Any officer receiving a Data Protection request direct should forward it immediately to Gary Cordes, Legal Services Manager. Extension No: 7906. Email: Gary.Cordes@thanet.gov.uk

4. All responses will be managed by Gary Cordes, Legal Services Manager

5. The information will be provided within a 40-day period, which commences once the Council is satisfied that all the necessary information has been received

Is there any other legislation that I must know about when considering a request for information?

The DPA is complemented by the Freedom of Information Act (2000). It is quite possible that a single request from the public may require both the Freedom of Information Act (FOI) and the Data Protection Act to be applied to it.

Simply put, if an individual or organisation requests information that is not personal data, but relates to a Public Authority, then the Freedom of Information Act 2000 applies.

If the request is for, or includes personal data, then the Data Protection Act must be applied.

Are there Penalties for Breaching the Data Protection Act?

Yes, One Local Authority was recently fined £100,000 by the Information Commissioners for wrongly disclosing personal information.

Can an individual member of staff be prosecuted under DPA?

Yes. Each employee can be personally prosecuted for unlawful activities concerning misuse of personal data. TDC staff should make sure they have proper authorisation for everything they do with personal data.

Generally, you must be prepared to share any comments or information that you store about living individuals. You may be required to share the information with them. This applies to both electronic and manual paper records.

Are all electronically saved documents covered by the DPA?

Yes. Any saved electronic document (whether e-mail, word-processed, spreadsheet or database) which contains personal data will have to be disclosed if an Information Request is received regarding the data subject concerned. Manual data is also affected by the DPA.

What are the time-scales for responding to a data access request?

The DPA requires TDC to comply with Information Requests promptly and, in any event within 40 days from receipt of request or, if later 40 days from the day on which TDC has both the required fee and the necessary information to confirm the data subject's identity and to locate the data.

Is CCTV covered by the DPA?

Yes. CCTV is considered a means of collecting and processing personal data.

Are the use of photographs, videos and webcams covered by the DPA?

Yes. Photographs of staff and members of the public are also classes of personal data, which need to be obtained and used fairly in accordance with the DPA principles. It is especially important to gain the permission of the data subjects before making their image publicly available, e.g. by putting them on the Internet.

Does the Council charge for requests under the Data Protection Act?

The Council charges a fee of £10 for responding to any Data Information Request.

If you have any questions about the Data Protection Act then speak to Gary Cordes, Legal Services Manager. Extension No: 7906. Email: Gary.Cordes@thanet.gov.uk

Contact Us

Data Protection Officer:
Harvey Patterson, Corporate & Regulatory Services Manager

Deputy Data Protection Officer:
Gary Cordes, Legal Services Manager

E-mail: Gary.Cordes@thanet.gov.uk

Tel: 7906.

See Also

The Information Commissioner's Office:
http://www.ico.gov.uk/

Thanet District Council's Policy & Procedures

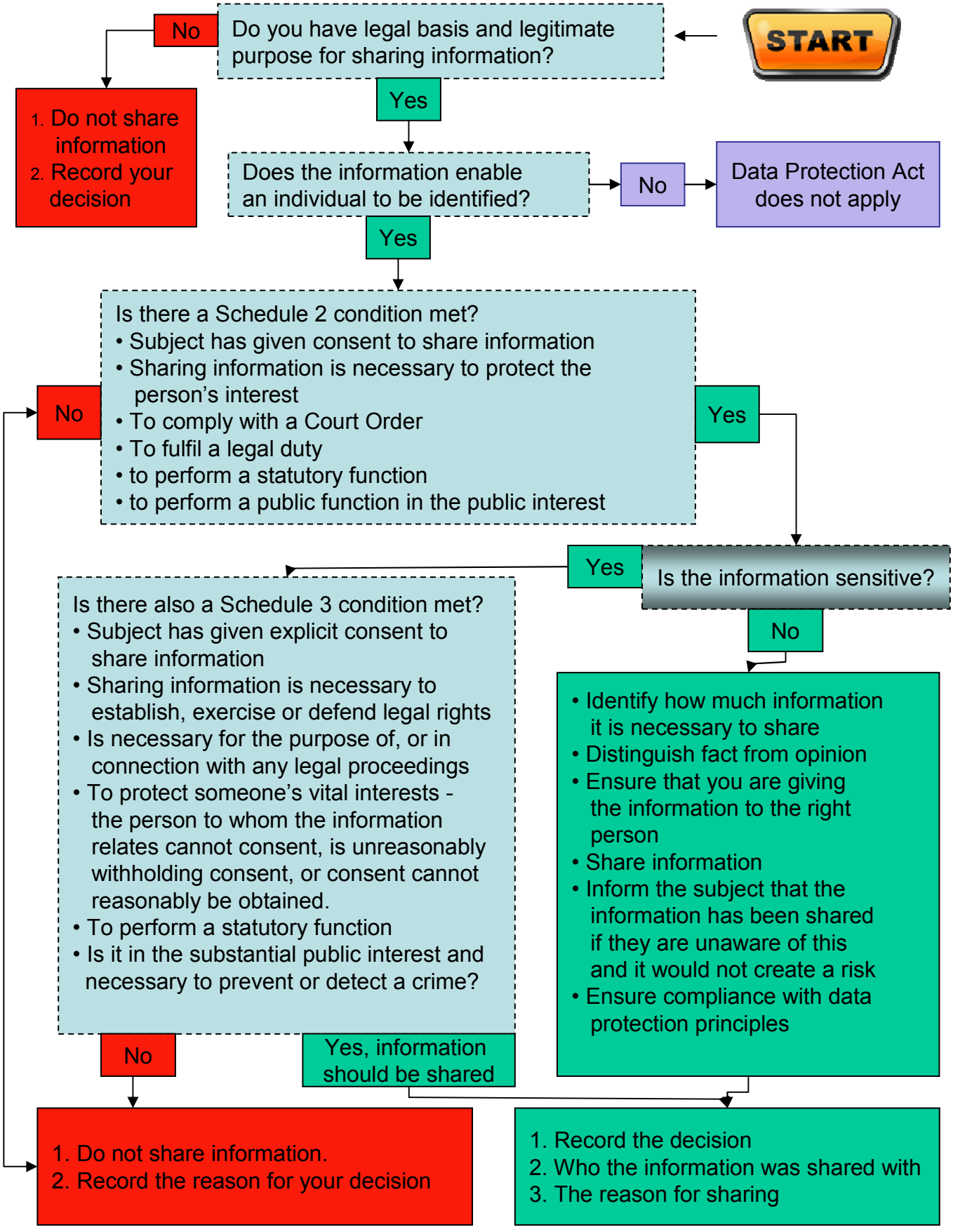
Data Protection Checklist

Subject Access Request Form

Breach Policy & Procedure

The Data Protection Act

Managers Guide to Sharing Information



This page is intentionally left blank

'HOW TO COMPLY' CHECKLIST

This checklist will help you comply with the Data Protection Act. Being able to answer 'yes' to every question does not guarantee compliance, but it should mean that you are heading in the right direction.

☐ **Yes** ☐ **NO** Do I really need this information about an individual?

☐ **Yes** ☐ **NO** Do I know what I'm going to use it for?

☐ **Yes** ☐ **NO** Do the people whose information I hold know that I've got it, and are they likely to understand what it will be used for?

☐ **Yes** ☐ **NO** Am I satisfied the information is being held securely, whether it's on paper or on computer? And what about my website? Is it secure?

☐ **Yes** ☐ **NO** Am I sure the personal information is accurate and up to date?

☐ **Yes** ☐ **NO** Do I delete/destroy personal information as soon as I have no more need for it?

☐ **Yes** ☐ **NO** Is access to personal information limited only to those with a strict need to know?

☐ **Yes** ☐ **NO** If I want to put staff details on our website have I consulted with them about this?

☐ **Yes** ☐ **NO** If I use CCTV, is it covered by the Act? If so, am I displaying notices telling people why I have CCTV? Are the cameras in the right place, or do they intrude on anyone's privacy?

☐ **Yes** ☐ **NO** If I want to monitor staff, for example by checking their use of email, have I told them about this and explained why?

☐ **Yes** ☐ **NO** Have I trained my staff in their duties and responsibilities under the Act, and are they putting them into practice?

☐ **Yes** ☐ **NO** If I'm asked to pass on personal information, am I and my staff clear when the Act allows me to do so?

☐ **Yes** ☐ **NO** Would I know what to do if one of my employees or individual customers asks for a copy of information I hold about them?

☐ **Yes** ☐ **NO** Do I have a policy for dealing with data protection issues?

☐ **Yes** ☐ **NO** is my notification up to date, or does it need removing or amending?

This page is intentionally left blank

Data Protection Act 1998

Data Protection

Introduction

Thanet District Council provides a wide range of services to many people. The Council may record information about you and the services that you receive.

What is the Data Protection Act 1998?

The **Data Protection Act 1998** (the Act) is designed to protect personal data. This covers information about any person, no matter how it is used, what it is used for or who uses it.

How does it protect personal data about you?

The Act sets rules and conditions which organisations must obey when gaining and using information about you. The Act also provides you with certain rights, which must be respected.

What are your rights to accessing your personal records?

- To ask the Council if it holds personal information about you
- To request a copy of that information
- To ask for incorrect personal information to be corrected
- To be given details about the purposes for which the Council uses the information and of other organisations or persons to whom it is given.

Why does the Council keep personal information?

So that the Council can provide you with the services you require. For example, the Council administers council tax, benefits, planning and housing services and needs to maintain a record of the services provided.

Anyone with whom the Council has contact may need to give some basic information about themselves, and their personal and family circumstances. Some people also have to give information about their financial situation. This information is put into a file. Other information can be added, for example, if the Council receives information from a doctor or teacher. The file will also include information that you and the relevant service have talked about.

Does the Council need your consent to use information about you for any of these purposes?

In normal circumstances we will ask your consent to use your personal information. However, there are some situations where the law requires us to use information without your consent.

How do you ask to see information about you?

When you want to see your records you need to:

- Write to the Deputy Data Protection Officer at the address at the end of this guidance
- or complete a Subject Access Request Form online and send to the Deputy DPO
- Pay a fee of £10

- Provide the Council with proof of your identity, and proof of your address and details of the information you require.

What information will you receive?

You are entitled to:

- copies of information that the Council holds about you on both computer and paper records
- a description of the purposes for which the Council uses your information
- a list of others who may have seen the information. This will be provided within a 40-day period, which commences once the Council is satisfied that all the necessary information from you has been received.

Is there any information that you cannot see?

Information is given to the Council by lots of different people and sometimes this information is given in confidence. The Council must respect the wishes of these people and therefore would need to ask their consent to release this information to you. Confidential information can include that given to the Council by doctors, the police, teachers and members of the public. The Council can only withhold information according to exemptions in the Data Protection Act. For example, where it is decided that disclosing information may cause someone to suffer serious harm, the Council may refuse to give this information.

Can other people see your file?

Other people, including members of your family, cannot see your file without your agreement. Likewise, you cannot see information about members of your family without their permission. However those with parental responsibility may see the files of those children who are not of an age to have an understanding of their files. This is on the understanding that the child has not given information that they expect to be kept confidential.

How will you be given the information?

You are entitled to be given a copy to keep and check for accuracy. This will either be a printout from a computer, a photocopy of the paper records or in electronic format if you prefer.

What if you think the information is wrong?

If you think any information recorded about you is wrong, you should inform a member of staff or tell the Council straight away. If the Council does not agree that the information is wrong, you can ask to record your disagreement on your records. You can also appeal to the Information Commissioner or through the courts if the Council does not correct the information. More details can be obtained by contacting the Information Access Officer at the address at the end of this guidance.

What do you do if you think you have not been given all of the information you asked for?

You can contact the Information Access Officer, appeal to the Council through its appeals and complaints procedure or you can appeal to the Information Commissioner. The Commissioner's staff will look into the matter on your behalf.

What if the Council has breached the Act?

If the Council has broken any of the rules or conditions established by the Act and you have suffered damage or distress you may be able to claim compensation. You may also be able to claim compensation if the damage or distress was caused by the Council's processing of your information. Claims are made through the Court. You must be able to prove that the Council had not taken reasonable care.

Contact

By Post: Deputy Data Protection Officer, Legal Services, Thanet District Council, PO Box 9, Cecil Street, Margate, CT9 1XZ

By telephone: 01843 577906

By E-mail: Gary.Cordes@thanet.gov.uk

This page is intentionally left blank

Thanet District Council

How we use your information

What you need to know

- why information is collected about you
- ways in which this information may be used
- what other agencies may have access to your information

www.thanet.gov.uk

Introduction

Thanet District Council asks for personal information so that we can ensure that customers receive the information, advice and services that are right for you. Information about you and the services you receive may be recorded, either on paper or computer files as part of providing you with council services.

At the time of collecting your information, the council will inform you for what purpose you provided it. It will also only collect the minimum information necessary to fulfill that purpose. When it no longer has a need to keep information about you, it will be disposed of in a secure manner.

How we protect your information

Sharing of information is strictly governed by information protocols and our codes of practice for confidentiality. These are produced in accordance with legislation and good practice and are designed to protect your rights. All our staff are required to work within these guidelines.

Sharing information with others

Please note that the council is required to share your information on occasion with third parties, such as agencies that help reduce crime or investigate fraud. Anyone who receives service user identifiable information from us is also under a legal duty to keep it confidential.

In particular, it will use information about you on the following basis:

- For all law enforcement, regulation and licensing, criminal prosecutions and court proceedings, the council will use all the information it holds to undertake those functions efficiently and effectively. The council may also need to share your personal and sensitive information with other councils and partner agencies.
- For all uses of information relating to situations where money is owed to the council or the council is making a payment in response to a claim for grants, housing or council tax benefits, your personal information (other than just your name, address, dates of occupancy etc) will be kept secure and used only for that range of purposes (and for the reasons stated above).

Service Delivery

By processing your personal data in this way, the council can ensure that it is able to:

- Provide you with a better level of service, ensuring that its information about you is accurate and up to date;
- Ensure that public money is spent wisely and efficiently;
- Avoid people being paid money to which they are not entitled;
- Avoid having to ask people to pay money back when it has been paid to them incorrectly;
- Reduce fraud and crime generally.

Your Rights

Under the Data Protection Act 1998, you have right of access to information we hold about you. A £10 fee is charged for this service. To apply for access to your information you should contact the Data Protection Officer at Thanet District Council.

If you think that any information that we hold about you is inaccurate, you can ask for the changes to be made.

Further information

To find out more on how we use your information, or if you would like a copy of this leaflet in large print, Braille, audio format or other languages, please contact:

The Data Protection Officer
Thanet District Council
PO Box 9
Cecil Street
Margate
CT9 1XZ

More information about Data Protection can be found at : www.thanet.gov.uk

This page is intentionally left blank

Privacy Statement

Data Protection Act 1998

Under the Data Protection Act 1998, we have a legal duty to protect any personal information we collect from you.

- We will only use personal information you supply to us for the reason that you provided it for.
- We will only hold your information for as long as necessary to fulfil that purpose.
- We will not pass your information to any other parties (including other Council departments) unless this is made clear to you at the time you supplied it.
- All employees and contractors who have access to your personal data or are associated with the handling of that data are obliged to respect your confidentiality.

Cookies and IP addresses

A cookie is a piece of information that is stored on your computer's hard drive by your web browser. We do use cookies to make it easier for you to complete on-line forms and questionnaires but these are only temporary and do not identify you or your visit to our site. However, the computers which host our website do maintain site logs which include the IP address details of all machines accessing our pages. This enables us to monitor website usage so we can

- See which pages are the most popular
- See which pages are seldom or never visited
- See how extensively the Council Website is used
- Publish a **summary of the above statistics to fulfil e-Government strategies**

Any IP information is treated as strictly confidential and is not published or divulged to any third party.

If you have any query about personal information that we may hold, please write to:

Gary Cordes
Deputy Data Protection Officer
Thanet District Council
PO Box 9
Cecil Street
Margate
CT9 1XZ

Email: Gary.Cordes@thanet.gov.uk

Copyright

Disclaimer

Every effort has been made to ensure the information contained on this website is correct and up to date, including hyperlinks to other organisations' websites. However, as the information on these sites is not maintained by the Council;

- We cannot accept responsibility for errors or omissions
- We do not necessarily endorse views or opinions expressed within these sites
- We cannot guarantee that any of these external links will work all of the time

This page is intentionally left blank

ST JOHN'S LODGE, ST JOHNS'S CEMETARY, MARGATE

To: **Cabinet Meeting - 23 June 2011**

Main Portfolio Area: **Economic Development and Regeneration**

By: **Mark Seed, Commercial Services Manager**

Classification: **Unrestricted**

Summary: **In accordance with the Asset Management Strategy, the above property was identified and approved of, for disposal by Cabinet on 5th August 2010. It was considered that the most likely use would be residential and Cabinet approved of a disposal for residential use. However, no offers for residential use have been received but a stone mason has made an offer to purchase the building in connection with his profession. The cabinet decision needs amending to reflect this.**

For Decision

1.0 Introduction and Background

1.1 As indicated above, it was contemplated that a residential bid would be the most likely offer to come forward, for the purchase of this property. No such offer was received but a stone mason has made an acceptable offer, to use the building in connection with his profession.

The company already do work at the cemetery and believe that on site representation will enhance their business opportunities. Clearly the use of the building by a monumental mason, is more compatible than a residential use.

2.0 The Current Situation

2.1 The market has been tested and an acceptable offer has been accepted, subject to contract, on behalf of the Council.

The building is currently used for office storage and the prospective purchaser also intends to use the building for offices.

On instructing solicitors, it was noted that Cabinet had technically agreed to a disposal for residential development and that this would need to be regularised.

3.0 Options

3.1 Revise the decision to allow for a disposal, without specific reference to use, as this would be covered by any planning requirements, if the prospective purchaser sought to change the use.

3.2 Endorse the existing decision.

4.0 Corporate Implications

4.1 Financial

4.1.1 If the existing decision is not amended, it is unlikely that the sale will proceed, which will result in a loss of a capital receipt, at least in the short term.

4.2 Legal

4.2.1 There are no considerations under this heading.

4.3 Corporate

4.3.1 The disposal is in accordance with the Council's Asset Management Strategy 2006-2011 and conforms with good asset management practice.

4.4 Equity and Equalities

4.4.1 There are no matters to consider under this heading.

5.0 Recommendation

5.1 That Cabinet modify the decision of 5.8.2010 to allow for a disposal without specific reference to use.

6.0 Decision Making Process

This is non-key decision that can be taken forward by Cabinet.

Contact Officer:	Justin Thomson, 7053
Reporting to:	Mark Seed

Background Papers

Title	**Details of where to access copy**
Potential Asset Disposal for 2010/2011Asset Management Cabinet 5.8.2010-Minutes	*TOM*

Exclusion of Public and Press

To:	**Cabinet Meeting - 23 June 2011**
By:	**Democratic Services and Scrutiny Manager**
Classification:	**Unrestricted**
Ward:	**N/A**

Summary: This report seeks the Committee's approval to exclude the public and press from the meeting on agenda item 10 as it contains exempt information as defined in Paragraphs 5 and 6 of Schedule 12A of the Local Government Act 1972 (as amended).

For Decision

1.0 Introduction

The public must be excluded from meetings whenever it is likely in view of the nature of the business to be transacted or the nature of the proceedings that confidential or exempt information would be disclosed.

Exempt information – discretion to exclude public

Subject to Article 6 of the Human Rights Act 1998 (right to a fair trial) the public may be excluded from meetings whenever it is likely in view of the nature of the business to be transacted or the nature of the proceedings that exempt information would be disclosed.

Meaning of confidential information

Confidential information means information given to the Council by a Government Department on terms which forbid its public disclosure or information which cannot be publicly disclosed by Court Order.

2.0 Exempt information

The full rules are set out in Part V and Schedule 12A Local Government Act 1972 (as Amended) and the Relevant Authorities (Standards Committees) Regulations 2001.

3.0 Reason for Exempt Item

The report author has classified Agenda Item 10 as disclosing exempt information under Paragraphs 5 and 6 of Schedule 12A of the Local Government Act 1972 (as amended) thereby excluding the press and public from the meeting whilst this item is debated.

4.0 Corporate Implications

4.1 Financial

There are no direct financial implications.

4.2 **Legal**

As per Schedule 12A of the Local Government Act 1972 (as amended)

4.3 **Corporate**

None

4.4 **Equity and Equalities**

There are no specific equity and equality considerations that need to be addressed in this report.

5.0 Recommendation

That the public and press be excluded from the meeting on agenda item 10 as it contains exempt information as defined in Paragraphs 5 and 6 of Schedule 12A of the Local Government Act 1972 (as amended).

6.0 Decision Making Process

This Committee must agree the recommendation if the press and public are to be excluded.

Contact Officer:	Glenn Back, Democratic and Scrutiny Manager
Reporting to:	Harvey Patterson, Corporate & Regulatory Services Manager and Monitoring Officer

Corporate Consultation Undertaken

Finance	Sarah Martin, Financial Services Manager
Legal	Harvey Patterson, Corporate & Regulatory Services Manager and Monitoring Officer

By virtue of paragraph(s) 5, 6 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

THANET DISTRICT COUNCIL DECLARATION OF INTEREST FORM

Do I have a personal interest?

You have a **personal interest** in any business of your authority where it relates to or is likely to affect:

a) An interest you must **register**.
b) An interest that is not on your register, but where the well-being or financial position or you, members of your family (spouse; partner; parents; in laws; step/children; nieces and nephews), or people with whom you have a close association (friends; colleagues; business associates and social contacts that can be friendly and unfriendly) is likely to be affected by the business of your authority more than it would affect the majority of**:**

- Inhabitants of the ward or electoral division affected by the decision (in the case of the authorities with electoral divisions or wards.)
- Inhabitants of the authority's area (in all other cases)

These two categories of personal interests are explained in this section. If you declare a personal interest you can remain in the meeting, speak and vote on the matter, unless your personal interest is also a prejudicial interest.

Effect of having a personal interest in a matter

You must declare that you have a personal interest, **and the nature of that interest**, before the matter is discussed or as soon as it becomes apparent to you except in limited circumstances. Even if your interest is on the register of interests, you must declare it in the meetings where matters relating to that interest are discussed, unless an exemption applies.

When an exemption may be applied

An exemption applies where your interest arises solely from your Membership of, or position of control or management on:
1. Any other body to which you were appointed or nominated by the authority.
2. Any other body exercising functions of a public nature (e.g. another local authority)

Is my personal interest also a prejudicial interest?

Your personal interest will also be a **prejudicial interest** in a matter if all of the following conditions are met:

a) The matter does not fall within one of the **exempt categories** of decisions
b) The matter affects **your financial interests** or relates to a **licensing or regulatory matter.**
c) A member of public, who knows the relevant facts, would **reasonably think your personal interest is so significant** that it is likely to prejudice your judgement of the public interest.

What action do I take if I have a prejudicial interest?

a) If you have a **prejudicial interest** in a matter being discussed at a meeting, you must declare that you have a prejudicial interest as the nature of that interest becomes apparent to you.
b) You should then leave the room, **unless members of the public are allowed to make representations, give evidence or answer questions about the matter**, by statutory right or otherwise. If that is case, you can also attend the meeting for that purpose.
c) However, you must immediately leave the room once you have finished or when the meeting decides that you have finished (if that is earlier). You cannot remain in the public gallery to observe the vote on the matter.

d) In addition you must not seek to **improperly influence** a decision in which you have a prejudicial interest.

This rule is similar to your general obligation not to use your position as a Member improperly to your or someone else's advantage or disadvantage.

What if I am unsure?

If you are in any doubt, Members are strongly advised to seek advice from the Monitoring Officer or the Democratic Services Manager well in advance of the meeting.

DECLARATION OF PERSONAL AND, PERSONAL AND PREJUDICIAL INTERESTS

MEETING……...

DATE…… **AGENDA ITEM** ……

IS YOUR INTEREST:

PERSONAL □

PERSONAL AND PREJUDICIAL □

NATURE OF INTEREST:

……

……

……

NAME (PRINT): ……

SIGNATURE: ……

Please detach and hand this form to the Committee Clerk when you are asked to declare any interests.