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 ……