

---

<b>Report To:</b>	<b>Policy &amp; Resources Committee</b>	<b>Date:</b>	<b>05 February 2013</b>
<b>Report By:</b>	<b>Head of Legal &amp; Democratic Services</b>	<b>Report No:</b>	<b>LA/932/13</b>
<b>Contact Officer:</b>	<b>Elaine Paterson</b>	<b>Contact No:</b>	<b>01475 712139</b>
<b>Subject:</b>	<b>Data Protection Policy</b>		

---

## **1.0 PURPOSE**

- 1.1 The purpose of this report is to seek the approval of the Policy & Resources Committee to the draft Data Protection Policy which forms Appendix 1 hereto.

## **2.0 SUMMARY**

- 2.1 The purpose of the Data Protection Act 1998 is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge and, wherever possible, is processed with their consent.
- 2.2 An important element in demonstrating the Council's commitment to compliance with Data Protection principles is having in place a Corporate Data Protection Policy.
- 2.3 Inverclyde Council's current Data Protection Policy was approved on 3 April 2003. It is now appropriate to revise and update the Policy to take account of the many developments since the original Policy was approved.
- 2.4 The Data Protection Policy has been revised and a draft thereof is attached hereto for consideration and comment.

## **3.0 RECOMMENDATIONS**

- 3.1 It is recommended that Members approve the draft Data Protection Policy.

Elaine Paterson  
Legal & Democratic Services

## **4.0 BACKGROUND**

- 4.1 Inverclyde Council is committed to a policy of protecting the rights and privacy of individuals (including customers, staff and others) in accordance with the Data Protection Act. The Council regards the lawful and correct treatment of personal information as important to its successful operation and to maintaining confidence between the Council and those with whom it carries out business.
- 4.2 The Public Records (Scotland) Act 2011 requires public authorities to review their practices in managing information and to produce a Records Management Plan requires organisations to have in place a Data Protection Policy approved by the Council.
- 4.3 In terms of the Act, the Council is a Data Controller.
- 4.4 Data Controllers are required to renew their notification with the Information Commissioner on an annual basis. The Council's notification is reviewed and maintained by the Head of Legal & Democratic Services.
- 4.5 The Commissioner has powers to audit and assess compliance with the Act and issue enforcement notices and financial penalties in cases of poor performance. Some of Scotland's local authorities have been through this process but, to date, Inverclyde Council has not been the subject of an audit.
- 4.6 The Council has in place policies and procedures which support compliance with the requirements of the legislation. However, these generally need to be reviewed and updated. The Information Governance Group is undertaking part of this process and the revision of the Data Protection Policy is one of the steps in that process.
- 4.7 The Data Protection Policy aims to support compliance with the requirements of the Data Protection Act and to promote awareness of the Council's responsibilities.
- 4.8 The Policy applies to all staff and Elected Members of the Council and it clarifies the roles and responsibilities in relation to Data Protection. The Policy also applies to external partners and agencies that may be processing information on behalf of the Council, either in terms of a contractual arrangement or because the Council requires to share information with them.
- 4.9 Elected Members and staff will be provided with appropriate guidance, training and procedures to aid compliance with this Policy and with their wider responsibilities in terms of the legislation.

## **5.0 PROPOSALS**

- 5.1 The Data Protection Policy establishes and confirms the Council's compliance with the requirements of the Data Protection Act. The proposed Policy is attached at Appendix 1 to this report.
- 5.2 The Data Protection Policy provides a framework that manages the risks associated with processing personal data and supports service delivery.

## **6.0 IMPLICATIONS**

- 6.1 Financial Implications - there are no financial implications.

# **Inverclyde Council**

## **Data Protection Policy**

## **1. Policy Statement**

- 1.1 Inverclyde Council ('the Council') collects and processes personal information about its customers, staff and others to allow the Council to carry out many of its functions and responsibilities. This personal information, however it is acquired, held, processed, released or destroyed, must be dealt with lawfully and appropriately in accordance with the Data Protection Act 1998 ('the Act').
- 1.2 Dealing appropriately with personal information will not only ensure that the Council complies with its legal obligations but will contribute to maintaining the confidence of customers, staff and others.
- 1.3 The Council is committed to protecting the rights and privacy of individuals, be they customers, staff or others, in accordance with the Act and to this end will promote a culture of awareness of the Act.
- 1.4 To comply with the law, information about individuals must be collected and used fairly, stored safely and securely, retained no longer than is necessary and not disclosed to any third party unlawfully.
- 1.5 This Policy applies to all staff and Elected Members of the Council. Any breach of the Act or the Council's Data Protection Policy is considered to be a disciplinary offence and disciplinary procedures will apply.
- 1.6 Other agencies and individuals working with the Council, and who have access to personal information, are required to have read this Policy and comply with its terms.
- 1.7 Services who deal with external contractors processing Council information are responsible for ensuring that such agencies sign a contract agreeing to abide by this Policy and which contains robust conditions designed to protect personal data.
- 1.8 This policy applies to all situations where the Council processes (collects, stores, uses, shares) personal data about living individuals. It includes information stored in any format including but not limited to personal data held:
  - electronically;
  - on paper;
  - on CCTV;
  - in photographs; and
  - on audio equipment.

## **2. Data Protection Act 1998**

- 2.1 The purpose of the Act is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent.
- 2.2 Appendix 1 hereto sets out the eight Data Protection Principles ('the Key Principles') defined in the Act.

## **3. Responsibilities**

- 3.1 The Council is the data controller under the Data Protection Act.

- 3.2 The Corporate Management Team, Chief Officers and Service Managers are responsible for developing and encouraging robust information handling practices.
- 3.3 Compliance with data protection legislation is the responsibility of all staff and Elected Members who process personal information.
- 3.4 Each Service and its senior management shall retain a service responsibility for compliance with the provisions of the Act and this Policy. All Services will nominate an officer whose role will be to monitor compliance within their Service, to pass on advice and training, to maintain the accuracy of their Service's input into the Council's Notification to the Information Commissioner and to ensure that subject access requests are properly and timeously processed.
- 3.5 All staff will be responsible for following procedures and systems for maintaining appropriate security of the personal data to which they have access.
- 3.6 From time to time, Services shall monitor their compliance with the Council's policies, procedures and guidelines and review their security arrangements.
- 3.7 The Corporate Management Team will ensure that staff are provided with guidance, training and procedures to promote a culture of compliance with the Act and with this Policy.

#### **4. Implementation of Key Principles**

- 4.1 In complying with the key principles of the Act set out in Appendix 1, the following practices will be applied:-
  - (a) The Council will process data in relation to its employees, clients and customers, and business partners in accordance with the Council's Notification to the Information Commissioner's Office (ICO);
  - (b) All sharing of personal data with other organisations will be appropriately documented. Where the sharing is voluntary (rather than a statutory requirement) a prior written agreement will be in place;
  - (c) When personal data is collected the Data Subject will normally be provided with a Privacy Notice, providing information about what we collect, why this information is needed and how it will be processed. Any exceptions to this will be documented;
  - (d) The Council will identify and collect the minimum amount of information that is necessary for the purpose. If it becomes necessary to hold or obtain additional information about certain individuals, such information will only be collected and recorded in relation to those individuals;
  - (e) The Council will adopt policies that ensure that all relevant information is kept accurate and up to date. Where the Council identifies an inaccuracy or a Data Subject indicates that information held by the Council or a business partner is inaccurate, the error will be rectified by the owner of the data;
  - (f) The Council will implement procedures in relation to the retention of personal data in accordance with the Corporate Records Retention Schedule;

- (g) Requests for Subject Access must be complied with within 40 days, subject to receipt of all necessary information and the appropriate fee;
- (h) Personal data will be appropriately safeguarded from accidental destruction, theft or any other loss; and
- (i) Where there is a requirement to take personal data off-site, procedures will be adopted to ensure the safe keeping of that data.

## **5. Notification**

- 5.1 The Information Commissioner maintains a public register of data controllers. The Data Protection Act 1998 requires every Data Controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.
- 5.2 Notification is the responsibility of the Head of Legal & Democratic Services. Corporate Directors are responsible for notifying and updating the Head of Legal & Democratic Services of the processing of personal data within their Service.
- 5.3 Details of the Council's notification are published on the Information Commissioner's website.
- 5.4 All proposed systems or systems under development which would process personal data must be checked prior to development to ensure that the processing will be covered by our DPA Registration.

## **6. Data Subject Rights**

- 6.1 Data Subjects have the following rights regarding data processing, and the data that are recorded about them:
  - To request information regarding the nature of information held and to whom it has been disclosed. This is referred to as the subject making a Subject Access Request;
  - To prevent processing likely to cause damage or distress;
  - To prevent processing for purposes of direct marketing;
  - To be informed about mechanics of automated decision making processes that will significantly affect them;
  - Not to have significant decisions that will affect them taken solely by automated process;
  - To take action to obtain compensation if they suffer damage by any contravention of the Act;
  - To take action to rectify, block, erase or destroy inaccurate data;
  - To request the Commissioner to assess whether any provision of the Act has been contravened;
- 6.2 The Council shall ensure that the rights of Data Subjects are respected.

## **7. Consent**

- 7.1 Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. In most instances consent to process personal and sensitive data is obtained routinely by the Council. Forms

that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed.

## **8. Disclosure of Data**

8.1 The Council must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff and Elected Members should exercise caution when asked to disclose personal data held on another individual to a third party.

8.2 Personal data may be legitimately disclosed where one of the following conditions apply:

- The individual has given their consent;
- The disclosure is in the legitimate interests of the Council;
- The Council is legally obliged to disclose the data;
- The disclosure of data is required for the performance of a contract;
- The Act permits disclosure.

## **9. Review      Date**

9.1 This Policy will be reviewed in every fourth year following its adoption.

## **10. Conclusion**

10.1 The Council subscribes to the principles of the Act and will continue to develop policies, procedures and guidelines to ensure compliance with its legal obligations.

## **Appendix 1**

### **Data Protection Key Principles**

- (1) Personal data shall be processed fairly and lawfully.
- (2) Personal data shall be processed only for the purposes for which it was obtained.
- (3) Personal data shall be adequate, relevant and not excessive.
- (4) Personal data shall be accurate and kept up to date where necessary.
- (5) Personal data shall not be kept longer than necessary.
- (6) Personal data shall be processed in accordance with the rights of the Data Subject.
- (7) Personal data shall be secure.
- (8) Personal data shall not be transferred to countries which do not have adequate data protection systems, measures or laws.