# Internal Audit Report

**FINAL**

**Customer Services Department**

**Review of Data Protection**

**April 2010**

## 1 INTRODUCTION

This report has been prepared as a result of the Internal Audit review of Data Protection within the Corporate Services Department as part of the 2009 - 10 Internal Audit programme.

Discussions with Convention of Scottish Local Authorities (COSLA) in relation to the Information Commissioner's wider powers resulted in agreement that it would be helpful to undertake a review of the processing of personal data, within a Scottish Local Authority, to seek to determine any fundamental issues with regard to levels of compliance with the Data Protection Act 1998 (DPA). The intention was to identify key areas of non-compliance, which may be generic across all Scottish Local Authorities, and disseminate the lessons learned so that remedial action could be taken.

Argyll & Bute Council (A&BC) agreed to participate on a voluntary basis, in effect acting as a pilot local authority. (The Information commissioner had not identified any specific prior data protection failings by A&BC.)

In July/August 2009, the audit was conducted by the Information Commissioner's staff using Data Protection Audit Methodology. This methodology included:

- Adequacy Audit to review documented policies and procedures
- Compliance Audit involving:
  - On-site visit
  - Interviews with A&BC personnel who operate in the identified areas
  - Inspection of the associated records/evidence.

As a result of work carried out by the Information Commissioner's Office (ICO), it was considered that the current arrangements in place at A&BC in relation to compliance with the DPA with regard to governance and controls, provides a "Limited Assurance" that processes and procedures are in place and being adhered to. The objective of achieving data protection compliance is therefore threatened.

The ICO issued a final report 15 December 2009 specifying actions required to improve the adequacy and effectiveness of data protection governance and control. These actions were agreed and timetabled for completion.

## 2 AUDIT SCOPE AND OBJECTIVES

The overall objective of the audit will be to review the degree of implementation that has taken place regarding the actions outlined in the ICO report.

The broad objectives of the review were to ensure:

- Progress is being made in addressing the actions required

- Documentation is obtained to evidence actions addressed
- Actions not yet addressed are noted and new completion dates are obtained
- Prepare a report that outlines the current situation in respect of progress made by management in addressing the ICO actions

## 3 RISK ASSESSMENT

As part of the audit process and in conjunction with our Systems Based Auditing, ICQ approach, the risk register was reviewed to identify any areas that needed to be included within the audit.

Although the Strategic Risk Register recognises the loss of IT data, consideration should be given to developing a risk for data protection at operational risk register within departmental services.

## 4 CORPORATE GOVERNANCE

There are no Corporate Governance issues to be reported as a result of this audit.

## 5 MAIN FINDINGS

The recommendations identified on the Information Commissioner's report have been largely dealt with; however, there remain a number of actions still to be addressed.

## 6 RECOMMENDATIONS

Six recommendations were identified as a result of the audit of which five recommendations are classed as Medium and one Low. The recommendations are shown in the action plan below.

## 7 AUDIT OPINION

Based on the findings we can conclude that the reasonable progress is being made implementing the ICO report recommendations. However there are still some to be fully implemented. An action plan is provided in Appendix 2.

Recommendations arising from the audit work should be implemented by the nominated responsible officer within the agreed timescale. Recommendations not implemented will require explanation to the Audit Committee. This could lead to findings being reported in the Internal Control Statement produced by the Council in support of the Annual Accounts.

## 8 ACKNOWLEDGEMENTS

Thanks are due to the Data Protection and Information Officer for their co-operation and assistance during the Audit and the preparation of the report and action plan.

Argyll & Bute Council's Internal Audit section has prepared this report. Our work was limited to the objectives in section 2. We cannot be held responsible or liable if information material to our task was withheld or concealed from us, or misrepresented to us.

## APPENDIX 2 ACTION PLAN

| No. | ICO FINDINGS | PRIORITY | RECOMMENDATION | RESPONSIBLE OFFICER | IMPLEMENTATION DATE |
|---|---|---|---|---|---|
| **1** | A process to facilitate improvement in the current exception reporting is to be developed to support the controls required to demonstrate compliance with the DP policy framework. | Medium | The current process being developed to improve the existing exception reporting should continue. | Head of Governance and Law | 31 August 2010 |
| **2** | The Data Retention Schedule has not yet been finalised | Medium | It is recommended that the review and updating of the Data Retention Schedule is brought to a conclusion and published on the public folders for all staff to access. | Data Protection & Information Security Administrator | 30 June 2010 |
| **3** | The Data Protection Code of Practice contains no guidance for departments regarding the requirement to assess all new and revised policies/practices against DP legislative requirements and good practice. | Medium | The revised guidance should be completed and issued. | Data Protection & Information Security Administrator | 30 June 2010 |

| No. | ICO FINDINGS | PRIORITY | RECOMMENDATION | RESPONSIBLE OFFICER | IMPLEMENTATION DATE |
|---|---|---|---|---|---|
| **5** | The current Information Security Forum terms of reference is being updated | Medium | The Information Security Forum Terms of Reference should be reviewed and updated. Thereafter it should be placed on the Council's Public Folders. | Data Protection & Information Security Administrator | 31 May 2010 |
| **6** | Issues regarding staff training in Data Protection and Freedom of information are still to be addressed due to the current modernisation programme. | Medium | The Data Protection and Information Security Administrator should continue efforts in this area to ensure implementation by the end of August 2010. | Data Protection & Information Security Administrator and Learning Development Manager | 31 August 2010 |