OPERATIONAL MANAGEMENT GROUP

PRIVACY AND PUBLIC CONFIDENCE IN SCOTTISH PUBLIC SERVICES:
DRAFT IDENTITY MANAGEMENT AND PRIVACY PRINCIPLES

Background

1 On 31 August 2009 the Scottish Government opened a new consultation, “Privacy and Public Confidence in Scottish Public Services: Draft Identity Management and Privacy Principles”, setting out draft principles that identified key areas of guidance on identity management and privacy requirements in public bodies. The key issues underpinning the draft principles are that members of the public must be satisfied that public authorities and other organisations respect their privacy and recognise the harm that may be done if personal data are collected or held unnecessarily, lost or misused. It is expected that adherence to the draft principles will also help organisations comply with data protection and human rights legislation.

2 Responses to the consultation are due by 23 November 2009. The importance of the consultation is underpinned by new powers that the UK Information Commissioner will assume in April 2010, which will give his office the authority to fine organisations that do not process privacy and personal data in line with strengthened privacy requirements.

3 The objective of this paper is to:

   a) seek approval from the group to set up an identity management and privacy task force and to set out the remit of such a group
   b) bring the Scottish Government consultation recommendations to OMG’s attention

The full consultation can be viewed on the Scottish Government website:
http://www.scotland.gov.uk/Publications/2009/08/PrinciplesConsultation

The requirements of the Data Protection Act can be viewed on the UK Information Commissioner’s Office website:

Claire Turnbull Ext 86913
Timing

4 The final consultation report will be published in February 2010, so work on the requirements of the draft recommendations should be initiated as soon as possible, with implementation by April 2010 at the latest.

Discussion

5 The Scottish Government consultation draft principles and the recommendations identified by the UK Information Commissioner both contain requirements on personal data and privacy that are cross cutting and corporate in nature. The recommendations cover:

- proving identity and entitlement
- governance and accountability
- risk management
- data and data sharing
- education and engagement

6 Given the corporate nature of the identity management and privacy requirements set out by the Scottish Government consultation and by the ICO, OMG approval is sought for the development of an identity management and privacy task force, to be overseen by the FOI and data protection steering group.

7 The reason for setting up such a task force is that no single office has the capacity and expertise to develop and implement all the necessary corporate identity management and privacy requirements.

8 The remit of the task force, which will be chaired by Claire Turnbull, will be to:

- respond to the Scottish Government consultation;
- develop auditable policies and procedures in relation to privacy and data management;
- identify the personal data that we seek from our internal and external customers, identify how the data are used, identify any relevant changes in terms of the security of the data and
engagement with the data subjects, implement any changes and document them;

- update and broaden our data protection policy and guidance for SPCB staff and members;

- develop user-friendly guidance on our website so that members of the public understand how we will process their personal data;

- develop privacy impact assessments as part of the project planning process and provide relevant training and awareness;

- check all areas where there may be an impact on privacy, for example CCTV processes, and ensure compliance with the standards required by the consultation recommendations;

- identify areas where privacy could be affected by technology and ensure that risks are mitigated appropriately, for example by encryption of personal data, especially when data are processed remotely; and

- provide education and training on identity management and privacy principles for our staff and for our internal and external customers.

9 When a work plan has been developed by the identity management and privacy task force, progress will be overseen by the FOI and DP steering group.

Resource implications

10 There will be resource implications for the offices that provide knowledge and expertise to the task force. Initial considerations suggest that representatives should be included from offices that engage with members of the public and/or process data that may include identity management and privacy requirements.

11 We recommend that the following key offices or groups of offices provide at least one representative and that further expertise is drawn from additional offices as required:

- Business Information Technology, Security, Office of the Solicitor, Public Affairs Group, Human Resources and SPICe

12 We estimate that each representative would be involved in task force activity for one to two hours each week over six to eight weeks.

13 Implementation and review of the work carried out by the task force will be overseen by the FOI and DP steering group. It is expected that the
steering group will meet fortnightly while the work of the task force is under way.

Dependencies

14 FOI and DP steering group members have discussed the content of this paper and BIT, PAG and Security group/office heads have been consulted. The setting up of an identity management and privacy task force is contingent upon input from task force representatives and from FOI and DP steering group members.

Equalities implications

15 The Equalities Manager has been consulted: while there are no equalities impacts in relation to the development of an identity management and privacy task force, the remit of the task force should take account of all human rights legislation requirements and UK equalities legislation.

Publication scheme

16 This paper should be published under the publication scheme.

Next steps

17 Subject to approval from OMG, the next step is to set up the identity management and privacy task force and to agree its membership and remit.

Decision

18 OMG is invited to:

- agree that we set up a privacy and identity management task force as outlined in the paper;
- decide which key offices should be represented on the task force;
- nominate task force members by 16 October 2009;
- commit the necessary resources to the work.

SPICe
October 2009