



Report to Audit Sub-Committee

Date: 24 March 2010

Author: S M SALE – HEAD OF DEMOCRATIC & COMMUNITY SERVICES

Subject: ISSUE OF MONETARY PENALTIES BY THE INFORMATION COMMISSIONER

1. Purpose of the Report

To inform Members that the Information Commissioner [ICO] will have the power to impose a monetary penalty on the Council as a data controller for serious contraventions of the data protection principles from 6 April 2010.

2. Background

- 2.1 Sections 55A and 55B of the Criminal Justice and Immigration Act 2008 amended the Data Protection Act 1998 to enable the ICO to serve a monetary penalty notice on a data controller. It does not apply retrospectively therefore monetary penalty notices will only be used in respect of contraventions occurring on or after 6 April 2010.
- 2.2 A monetary penalty notice is a notice requiring a data controller to pay a monetary penalty of an amount determined by the ICO not exceeding £500,000.
- 2.3 A monetary penalty notice cannot be imposed on an employee. It will be served on the Council as data controller.
- 2.4 The ICO may impose a monetary penalty notice if a data controller has seriously contravened the data protection principles and the contravention was of a kind likely to cause substantial damage or substantial distress. In addition the contravention must either have been deliberate or the data controller must have known or ought to have known that there was a risk that a contravention would occur and failed to take reasonable steps to prevent it. Minor contraventions may still be subject to other enforcement procedures, such as an Undertaking, Enforcement Notice or prosecution.
- 2.5 The ICO has issued statutory guidance which will be taken into

account when determining whether to impose a Monetary Penalty. A copy of the guidance is available on the ICO's website and gives examples of the factors which will be taken into account when determining whether to impose a Monetary Penalty.

2.5.1 Example – serious contravention

The failure by a data controller to take adequate security measures (use of encrypted files and devices, operational procedures, guidance etc.) resulting in the loss of a compact disc holding personal data.

2.5.2 Example - substantial

Inaccurate personal data held by an ex-employer is disclosed by way of an employment reference resulting in the loss of a job opportunity for an individual.

2.5.3 Example - damage

Following a security breach by a data controller financial data is lost and an individual becomes the victim of identity fraud.

2.5.4 Example - distress

Following a security breach by a data controller medical details are stolen and an individual suffers worry and anxiety that his sensitive personal data will be made public even if his concerns do not materialise.

- 2.6 In determining the level of the monetary penalty, the ICO will take into account matters such as the nature of the contravention, effect of the contravention, what processes the data controller had in place to avoid the contravention, whether the data controller will gain financially and whether the penalty will have an adverse impact on the data controller. In relation to the latter, the ICO will take into account the sector (for example, whether the data controller is a voluntary organisation), the size, financial and other resources of a data controller before determining the amount of a monetary penalty. The purpose of a monetary penalty notice is not to impose undue financial hardship on an otherwise responsible data controller.
- 2.7 The process is fairly straightforward. The ICO must initially serve a notice of intent on a data controller first. The data controller has the opportunity to make written representations within 21 days. After considering those representations the ICO will serve the monetary penalty notice or take no action. If full payment is made within 28 calendar days of the monetary penalty notice being served, it will be reduced by 20%. If the penalty is not paid, it can be recovered by Order of the County Court or the High Court. A data controller on whom a monetary penalty notice is served may appeal to the Tribunals Service.
- 2.8 The introduction of the monetary penalty system reinforces the

importance of the Council meeting its responsibilities under the Data Protection Act. As Members are already aware, the Data Security Group is still working on a raft of policies to improve data security. In addition to this work has been continuing behind the scenes by IT to improve security.

- 2.9 Historically, data protection training has been provided by the Legal Section as part of “corporate issues” training. Although last year more detailed Data Protection Training was provided by the Senior Solicitor to specific departments. Planning Policy received training on 7 October 2009 and the majority of the Revenues and Benefits staff were trained on 23 and 27 November 2009. Feedback suggests that the training was well received. It is important that this training continues and is offered to all members of staff who have access to personal data. In order to facilitate this, training sessions have been set up throughout 2010 for all staff who wish to attend.

3. **Proposal**

That Members note the contents of the report.

4. **Recommendation**

It is therefore **recommended** that Members note the contents of the report.