ATODIAD / ENCLOSURE CH

Cyngor Sir Ynys Môn / Isle of Anglesey

COMMITTEE	Standards Committee
DATE	9th March 2011
TITLE OF REPORT	Review of access to back-office areas by Elected Members
REPORT BY	Huw Pierce Pritchard, Corporate Information Officer
PURPOSE OF THE REPORT	To advise the Standards Committee about the review of access rights to back-office areas and to accept the recommendations made.

Introduction

1. This report is produced at the request of the Interim Managing Director further to a review of the risks of the current access arrangements to Council offices where personal information is kept and used.

2. The review was undertaken by the Corporate Information Officer during November/ December 2010 following an apparent data breach arising from access to the offices of the Housing Service and complaints by officers about unauthorised access by Members to offices where sensitive personal information is used and stored.

3. Whilst the review made no distinction between Officers and Members and the findings of the report apply to County Councillors and Officers alike, this report considers the rights of access to offices by Councillors.

4. The review involved consultation with a range of other local authorities in England and Wales. Therefore this report takes into account statutory requirements and also best practice in the public sector.

5. A number of recommendations are made that are intended to ensure compliance with the Data Protection Act 1998 and mitigate against risks to the security of personal and confidential information.

Background

6. The Data Protection Act 1998 (DPA) is the main statutory driver for change in the way that personal data is gathered, stored and accessed. The DPA states that:

> *Appropriate technical and organisational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*

7. There are also other laws which relate to specific information which include offences. In addition, those affected by unauthorised access to and use of information can seek the traditional common law remedy for breach of confidence.

8. The DPA contains a number of offences and the Information Commissioner was given the power to fine organisations in April 2010.

9. In his Guidance, the Information Commissioner states that fines should be levied when actions are deliberate, involve an ignoring of risk and when they cause real distress. In November 2010 Hertfordshire County Council was fined £100,000 and a private sector company was fined £60,000 under those powers.

10. The Information Commissioner has stated that he will impose a monetary penalty notice where organisations seriously "*contravene the data protection principles and the contravention was of a kind likely to cause substantial damage or substantial distress*".

11. The review identified that the data breach involving the Housing Service could have resulted in enforcement action by the ICO and personal sanctions against the individuals involved.

12. The Council is obliged to review its organizational arrangements for the security of personal information and to take steps to prevent harm to individuals through breaches of the Act and to protect the Council from consequent monetary penalties.

13. The ICO expects that the Council will employ disciplinary sanctions in the event of deliberate misuse of information by Members or not complying with information security safeguards. Members should understand that deliberate misuse or reckless use of personal information may result in disciplinary action being taken.

14. In addition, the Council was the first local authority to sign up to the Information Commissioner's Personal Information Promise in 2009. The Promise is intended to help strengthen public trust and confidence in the way organizations handle their personal information. The Promise sets out that the Council will take robust disciplinary action where needed.

Access to offices.

15. Access to offices is currently provided by means of a swipe-card and Members are permitted access to most offices and meeting rooms. However, access by the public to offices is restricted.

16. The Council maintains a database of the use made of the swipe-cards to access areas. As part of the review the log for the swipe-card activated doors of the Housing Service was examined.

17. The log demonstrates that, between 1 January 2010 and 4 November 2010, 91 separate visits by Members were made to the Housing Service's back office areas. The figure does not include pre-arranged meetings between Members and Service staff in meeting rooms. This level of access to offices poses a level of risk that is not compatible with the requirements of DPA.

18. Extensive consultation with local authorities in Wales and England (November 2010) demonstrated that many Councils depend on their protocols and policies to limit visits of the

type and frequency demonstrated above. However, it is unlikely that self regulation could provide the solution to a problem that seems to be inherently cultural.

19. The Council controls access to certain areas where the risk of unauthorised access is perceived. This means that the bearer of a swipe card would require specific access rights in order to access the restricted area. Access to ICT and Human Resources is currently restricted. Access rights are controlled in these service areas primarily because of service specific best practice. However, the over-arching statutory requirement is the seventh data protection principle of the DPA.

20. The review took a risk based approach and established that service areas where highly sensitive and confidential personal information is processed presented the greatest risk for the Council. The areas identified are the Council's Housing Service; Social Services; Finance and Legal Services. These service areas can be accessed by any holder of a swipe-card regardless of whether that person has a legitimate business need.

21. Access to the high risk areas should be restricted as soon as possible to those with a legitimate business purpose for access. Members do not require access to these areas. It is not likely that removing the automatic and comprehensive access rights of Members would prove to be an obstacle to effective working.

22. Restricting access may pose some logistical difficulties, which are currently being investigated. It is likely that a staged process of restricting access would be most effective in the long term.

23. The costs of implementing the improvements are also being investigated.

24. Access arrangements to the Housing Service and Social Services should be addressed first. The remaining high risk services should be dealt with following discussion with service heads.

25. It is relevant that the areas identified above, with the exception of Legal Services, have reception areas and meeting rooms.

26. The revisions to the Member / Officer protocol seek to limit ad-hoc meetings in favour of pre-arranged meetings and briefings.

Conclusions

27. The Council should implement the necessary changes to its current arrangements in order to reduce the risk of data breach and heavy penalties for failing to comply with the Data Protection Act 1998 and best practice.

Recommendations

28. That the Council should restrict the current access rights of Members to the high risk service areas identified, namely the Housing Service, Social Services, Finance and Legal Services.

29. That the Council should prepare an appropriate protocol relating to the rights of access of Members to back-office areas for inclusion in the Constitution.