

DERBYSHIRE COUNTY COUNCIL

CABINET MEMBER MEETING – COUNCIL SERVICES

4 April 2014

Report of the Director of Transformation

Information Security Management (ISO 27001) Certification

1. Purpose of the Report

To provide an update on the work of the Information Governance Group specifically in relation to the County Council being accredited against the Information Security Management standard (ISO27001).

2. Information and Analysis

The importance of information security has grown significantly in recent years. It recognition of this the Information Governance Group (IGG) was formed to improve the Council's security policies and operating procedures. The IGG includes representatives from all service departments.

A key objective for the Group has been to achieve compliance with the Information Security Management Standard (ISO 27001). ISO 27001 is the defacto international standard on establishing, maintaining and improving information security policies and procedures.

The benefits of developing and using a compliant security framework include the Council being able to :

- maintain its trusted reputation with service users, staff and partner organisations in relation to the safe handling of personal and confidential information
- demonstrate, in the context of the array of relevant legislation, that it has taken appropriate action to comply with the law
- systematically protect itself from the dangers and potential costs of computer misuse, cybercrime etc;

- protect itself from the penalties, of up to £500,000, which can be imposed by the Information Commissioner for security breaches.

The new Council Plan also recognises that “Modern information and communication technology infrastructure is fundamental to encourage economic activity and to give local people better access to services.”

To comply with the ISO27001 standard it is not sufficient to have the correct policy documents in place, it is also necessary to demonstrate a high level of awareness in relation to information security issues and ensure that improvements to existing processes are fully implemented.

The IGG identified that an extensive communications exercise was required across the Council to ensure full understanding and compliance with the new policies. The “Data Demon” campaign was commissioned to help with the huge task of changing our culture and educating staff with regards to their responsibilities relating to handling data securely.

Having completed all the preparatory work the Council was assessed against the ISO27001 standard in September 2013 by a team of accredited external assessors. As anticipated with such a large and complex organisation, a number of minor issues were identified by the assessment team that needed to be addressed. A follow-up assessment visit took place in January 2014 and based on the remedial work that had been undertaken the assessors recommended the County Council for ISO 27001 certification.

The certificate No. IMS UK/01/0109860137, a copy of which is attached, was registered on 3rd March 2014 and expires on 1st September 2016. It is a requirement of the standard that external surveillance audits must take place on a regular basis. The first audit for the Council will take place between 22nd-25th April, 2014.

The scope of the County Council’s registration covers “**the protection of all information and data assets for the delivery of all council functions, services and activities, excluding schools**”. The Council is also permitted to use the Certification Logos on promotional material. To date we have been unable to identify any other council that has achieved ISO 27001 certification across its entire business.

To achieve ISO 27001 certification has required a huge amount of work to be undertaken in all departments which would not have been possible without the input, hard work, dedication and enthusiasm of members of the Information Governance Group and the support from Senior Management.

This certification is a significant achievement for the County Council in both operational and reputational terms and the County Council can celebrate an award that involves all members of staff and all Elected Members. It is an excellent example of the 'One Derbyshire – One Team' approach.

3. Financial Considerations

The costs of the surveillance audits, estimated at £3,000 will be met from existing Transformation Service budgets.

4. Considerations

In preparing this report the relevance of the following factors has been considered: financial, legal, prevention of crime and disorder, equality and diversity, human resources, environmental, health, property and transport considerations.

5. Key Decision

No.

6. Call-in

Is it required that call-in be waived in respect of the decisions proposed in the report? No

7. Background papers

Background papers are available from Jo White - Information Security Manager (Transformation Service) Extn: 32147

8. OFFICER'S RECOMMENDATION

That the Cabinet Member notes :-

1. That the County Council was certified as complying with the international Information Security Management standard (ISO 27001) on 3rd March 2014.
2. That the Council will be subject to regular surveillance audits during the current certification period which is due to expire on 1st September 2016.
3. That there will be an on-going requirement to communicate with service users, staff, Elected Members and partner organisations in relation to developments of the Council's Information Security policies and procedures.

David Hickman
Director of Transformation

Certificate Number:

IMS UK/01/0109860137

This is to certify that the Information Security Management System of:

Derbyshire County Council

of

**County Hall, Matlock
Derbyshire, DE4 3AG**

has been assessed and registered by
ACS Registrars Ltd against the following
Information Security Management Standard:

ISO 27001:2005

The scope of registration is:

"The protection of all information and data assets for the delivery of all council functions services and activities excluding schools. The assets protected are physical locations, hardcopy data, electronic data, council records, policies & procedures, software & licences and physical IT hardware. The boundaries of the Information security management system are the physical locations, authorised mobile workers and the endpoints of the organisational network. Supporting technology Includes server platforms, network devices, and organisational networks within the control of the Derbyshire County Council. In accordance with Statement of Applicability Ver 4"

Signed by: 

Date of initial assessment:	02/09/2013
Date of registration:	03/03/2014
Date reissued:	N/A
Date of expiry:	01/09/2016

Whilst all due care was exercised in carrying out this assessment, ACS Registrars Ltd accepts responsibility only for proven gross negligence. This certificate remains the property of ACS Registrars Ltd to whom it must be returned upon request. Certificate validity may be verified at the address below.

**ACS Registrars Ltd., Sovereign House,
29 Reddicap Hill, Sutton Coldfield,
West Midlands B75 7BQ, UK
tel. 0121-241-2299 fax. 0121-241-4623
www.acsregistrars.com**

