



Report of the Chief Officer (ICT)

Member Management Committee

Date: 16th December 2009

Subject: Report to provide an update on ICT Matters

<p>Electoral Wards Affected:</p> <input type="checkbox"/> Ward Members consulted (referred to in report)	<p>Specific Implications For:</p> <p>Equality and Diversity <input type="checkbox"/></p> <p>Community Cohesion <input type="checkbox"/></p> <p>Narrowing the Gap <input type="checkbox"/></p>
---	--

1.0 Purpose Of This Report

1.1 The purpose of this report is to provide a position statement on the ICT projects and services which will impact on elected members.

2.0 Background Information

2.1 There are a number of major ICT initiatives which will affect ICT service provision to elected members including the move to Microsoft, the development of a dedicated Case Management solution, the impact of a new service provider on the members PDA service and the implications of the Council's Information Security policy for the way that some members currently work.

3.0 Main Issues

ICE – Implementing the Collaboration Environment

3.1 Members will be aware that one of the issues of moving to Microsoft Outlook, Exchange and Sharepoint under the Collaboration project is that the new technology cannot support mail files that are larger than 2 Gigabytes. A mail archiving tool is being developed to allow members' historic mail to be stored in an alternative location but still be accessible through Microsoft Outlook just as if it was in the mail file. This solution provides the appearance that all mail is still in the mail file i.e. emails are searchable and can be replied to or forwarded.

3.2 Members may recall that at the October meeting Member Management Committee was asked to assist in communicating appropriate messages about the migration

across their groups. The messages included ensuring that members cooperated to ensure that the migration was as smooth as possible. Activities which required cooperation included completing the appropriate level of training and undertaking tasks requested including making their laptops and PCs upgraded in advance of the migration.

- 3.3 Whilst the majority of members have assisted in these processes, there are still a number of laptops and PCs which have not been upgraded. In order to gain access to Microsoft Outlook the upgrade of the equipment must take place. Failure to do so will at best, significantly increase the duration of the migration project and, at worst, could result in an email system being unavailable to those members. A list of those members' devices still to be upgraded is provided regularly to members of the ICT Reference Group.
- 3.4 Members will be aware that they have been contacted with a range of options around training to assist them in the move to Microsoft Outlook. A link to computer-based training has been provided to all and a number of Members have undertaken either classroom-based or alternative one-to-one training.
- 3.5 Several officers within Group Support have been trained to "Super User" level to support members and guidance is available on the Council's intranet via documents such as Frequently Asked Questions to assist both during the migration period and afterwards.
- 3.6 A number of members have undertaken significant housekeeping to reduce the size of their mail files in advance of the migration. Their efforts are appreciated as the smaller the mail file, the more quickly we are able to complete the migration process.
- 3.7 When a rollout schedule has been agreed, members will be contacted individually to make the arrangements necessary to migrate across to Microsoft Outlook and Exchange. In order for the migration to take place, members are required to undertake certain tasks including with respect to encrypted mails and delegated access rights. There is a defined migration process which members will be guided through.

Members Case Management system development

- 3.8 The Members Case Management solution has undergone further development and acceptance testing to ensure the functionality required is in place and working correctly.
- 3.9 A pilot of the Case Management is being undertaken by members of the ICT Reference Group and their associated Group Support Officers during December. Any issues identified during the pilot will then be fixed with the system being made available to all Members during January 2010.
- 3.10 A User Guide has been produced for use by Members and Group Support Officers. Training for the Group Support Officers involved in the pilot took place on 27th November 2009.
- 3.11 One to one training will be available for all Members upon request and will be provided by staff from the Project team. Computer Based Training will also be available for those who prefer this approach.

- 3.12 At the meeting on 13th November the Members ICT Reference Group agreed that live operational running will take place for 3 months prior to a formal review and identification of any issues and further developments required.
- 3.13 The system will continue to be available in the live environment whilst all enhancements or requests for change will be investigated, costed and discussed with the ICT Reference Group. Where there remains sufficient budget to complete all requirements, these will be undertaken. In the scenario where there is insufficient budget to address all requirements, these will either be prioritised by the ICT Reference Group or a business case will be produced to secure any additional budget required.

PDA (Personal Digital Assistant) Update

- 3.14 Members will be aware that the mobile phone service provider is Damovo with the network provider being O2.
- 3.15 Members who use Council-provided PDA devices are currently still on the Orange network but will transferred to the O2 network simultaneously with, or shortly after, the move to Microsoft under the ICE Project.
- 3.16 For those Members who currently have a TyTNII device, this will need to be “unlocked” and configured to operate on the O2 network. For those who currently use an M3100 device, this will need to be replaced. Members will be contacted individually to make the necessary arrangements
- 3.17 Members who currently use a M3100 device will have their device upgraded to the HTC Touch 3G.
- 3.18 This is also an opportunity for Members to review whether or not they require a PDA device.

Information Security

- 3.19 Significant work has been undertaken ensure that the Council has the appropriate measures in place to protect the Council’s information using best practice standards wherever possible. The policy has been developed in line with legislative and regulatory frameworks, and also is designed to support the Council plan.
- 3.20 An extract of the Council’s Information Security policy is provided below
- The Council recognises that information and information systems are valuable assets, which play a major role in supporting the organisation’s strategic objectives. Information security is important for ensuring the safe and secure transaction of information for Council business and the success of carrying out policy and administrative activities.
 - Information security is an integral part of information sharing, which is becoming increasingly important to achieving Council aims and objectives. The management of personal information has important implications for individuals and is subject to legal obligations under the Data Protection Act 1998. The consequences of information security failures can be costly, potentially embarrassing and time-consuming.

- The purpose of the Information Security policy is to provide a framework to govern rules and procedures that determine the Council's commitment to ensuring that its information assets are protected and secure.
- The Information Security Policy applies to information in all its forms, including,
 - Paper
 - Electronic Documents
 - E-Mails
 - Voicemail
 - Web 2.0 records such as wikis, blogs and discussion threads
 - Visual images such as photographs
 - Scanned images
 - Microform, including microfiches and microfilm
 - Audio and video tapes, DVDs and cassettes
 - Published web content (Intranet, Internet, Extranet)
 - Databases
- This policy will also apply to any documents created in any other format that may be introduced or used in the future.
- The policy covers information transmitted by post, by person, by electronic means and by oral communication, including telephone.
- The policy applies throughout the lifecycle of the information from creation, through storage and utilisation to its ultimate disposal.
- Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.
- The policy applies to all officers and Council Members and to other users associated with the Council. With regard to electronic information systems, it applies to use of Council owned facilities and privately/externally owned systems when connected to the Council network directly or indirectly.

- 3.21 The emphasis of much of the work we are doing in moving to new technologies, such as the migration to Microsoft is in order to provide more effective means of working collaboratively both across the organisation and with trusted partners. Paradoxically, this means that some users including some Councillors will need to change their working practices.
- 3.22 An example of this is that previously a small number of Councillors have had their emails automatically forwarded from their LCC account to a private account. Under the new security rules this is not permitted as it involves transferring emails to an uncontrolled "insecure" environment. In some cases the reason for why members have been forwarding mail has been because the service provided by the Council offering has not been good enough or means Councillors having multiple devices – one for Council business, one for their own businesses or place of work and sometimes even another personal set.
- 3.23 A further example is that personally-owned devices (PCs, laptops, PDAs) should not be used to store or process Council information. Whilst using such equipment can appear attractive in terms of convenience, it introduces risks to our information systems which we cannot manage adequately. Copies of data are no longer in our

control and there is an increased risk of infections by malware (viruses, worms, Trojans etc).

- 3.24 Practices such those described above contravene security best practice guidelines and whilst they will not be permitted, Corporate ICT Services will work with those affected in order to seek out alternative ways of working to minimise disruption.

Email System Administration

- 3.25 Members have previously sought clarity around the role of the System Administrator with respect to the Council's email system. Access to the appropriate servers and mail files is necessary for administration and support purposes. Examples of functions which the System Administrator performs at the request of the account holder include allowing delegated access rights to another individual and investigating unsolicited and inappropriate emails. All of these activities are formally recorded and the function is limited to certain key individuals, each of which has a unique, authenticated account and any actions are recorded in the form of an audit trail.

4.0 Implications For Council Policy And Governance

- 4.1 There are no implications for Council policy or governance.

5.0 Legal And Resource Implications

- 5.1 There are no legal or resource implications

6.0 Conclusions

- 6.1 Officers recognise the benefits of providing technical solutions to assist members in carrying out their roles. The projects included in this report are designed to provide members with enhanced technical support whilst adopting established best practice around risk and representing value for money to the Council.

7.0 Recommendations

- 7.1 Members are asked to note the content of this report.

Background Papers

Report to Member Management Committee in October 2009