Leeds CITY COUNCIL

Originator: Andy Keightley

Tel: 37 60003

Report of the Chief Officer (ICT)

Member Management Committee

Date: 16th February 2010

Subject: Report to provide an update on ICT Matters

Electoral Wards Affected:	**Specific Implications For:**
	Equality and Diversity ☐
	Community Cohesion ☐
☐ Ward Members consulted (referred to in report)	Narrowing the Gap ☐

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 several major ICT initiatives currently underway which will affect ICT service provision to elected members including the migration from Lotus Notes to Microsoft Outlook as part of the ICE (Implementing the Collaboration Environment) project, the transfer of the Members' PDA (Personal Digital Assistant) service to a new service provider and the development and roll-out of a technical solution to assist in the management of casework. Members have also previously sought clarity around the role of the system administrator with respect to their email accounts

3.0 Main Issues

<u>ICE – Implementing the Collaboration Environment. The move to Microsoft Outlook (including the migration of PDAs)</u>

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 in size.

3.2 A technical solution has been developed to allow members' historic mail to be stored and accessed through Microsoft Outlook. This means that all mail is still searchable and can be replied to or forwarded regardless of the size of the mail file or the age of the correspondence.

3.3 A migration process has been developed which addresses the complexity of transferring members' mail files from Lotus Notes to Microsoft Outlook with the least possible disruption to members themselves.

3.4 In order for the migration to take place, members were emailed asking them to undertake certain tasks including with respect to encrypted mails, changing folder names where necessary, preparing Contact details and organising delegated access rights. As far as possible these tasks were automated requiring Members to click on certain buttons contained within the notification email.

3.5 The process also involved members bringing their devices into the Civic Hall and picking them up two days later. This is primarily due to the length of time it takes to migrate mail files from one system to the other. The process also allows for the simultaneous migration (or replacement) of their PDAs as appropriate. This unfortunately necessitates Councillors being without access to their email accounts for up to 48 hours, however it does mean that they will be provided with a full technical solution and the actual migration process being managed as closely as possible. A range of dates has been made available to make the process as convenient as possible.

3.6 Dedicated resources were lined up to manage the process as expediently as possible including out of hours technical support which was be available until 9.00pm for the duration of the migration period.

3.7 A range of measures were also provided to offer functional support in the use of the new system including access to training, Frequently Asked Questions, guidance notes and support provided by specifically trained "Super Users" within the Group Support offices.

<u>Members Case Management system development</u>

3.8 The pilot of the Case Management solution commenced on 9th December 2009 involving Members of the ICT Reference Group and those officers who provide them with casework support.

3.9 Agreement was reached with the Members ICT Reference Group that the duration of the pilot was to be extended in order to test more complex cases. The majority of cases which presented themselves during the initial pilot period were largely weather-related due to the prevailing conditions. It was generally agreed that an extension to the pilot would allow for more diverse and longer running cases to be managed. This would facilitate the longer term testing of more complex cases to ensure that the appropriate notification and reminders worked as envisaged.

3.10 Due to the fact that the system will be utilised by all Councillors within the some of the Groups, the extension to the pilot also provides the opportunity include additional Councillors and associated support officers. The original scope of the project was that the system would be developed primarily to provide support to those Councillors who managed their own casework. The change in emphasis potentially provides a different set of issues emanating from the use of the system and so this element needed to be tested. To this end, an additional six Councillors

have been trained in the use of the system. Increasing the scope of the pilot allows for the testing of additional technical and operational aspects of the development

3.11 Work is underway to address some of the issues which were identified in the early stages of the pilot. An example of this is that e-mailing capabilities were limited and requirements have been determined in order to provide additional functionality.

3.12 Between the issuing of the agenda and this meeting, guidance will be sought from the Members ICT Reference Group with respect to dates for making the system available to all members.

3.13 As previously reported, the system will continue to be available in the live environment whilst enhancements or requests for change are 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 Reference Group or a business case will be produced to secure any additional funding required.

Email System Administration

3.14 Members have previously requested clarification around the duties and roles carried out by the email administrators within ICT Services and guidance on why and when an administrator would need access to members email accounts.

3.15 In the vast majority of cases an ICT Officer performs tasks at the request of the account holder. Examples include allowing delegated access rights to an officer providing administrative support 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.

3.16 In resolving such issues, the administrator does not usually need to access the members mail file itself but would instead just need to do a configuration change on the server. An example of this is in the case of a password reset.

3.17 There are a few occasions where access to a mail account may be required without the express consent of the account holder. Such access is governed by the provisions of RIPA (Regulation of Investigatory Powers Act, 2001), and instances fall into 2 categories:

- Directed Surveillance under RIPA, and
- Access to the account for management purposes

3.18 In the case of the former category, access to a mail account would be at the specific, formal request of the Monitoring Officer, for example, in the investigation of material pertaining to possible fraud or a breach of the Email Code of Practice contained within the Members ICT Usage Guidelines and which constitutes part of the Member Code of Conduct provisions. The relevant section of the Members ICT Usage Guidelines is attached at Appendix A.

3.19 An example of the latter is where someone has gone on holiday and another person needs a copy of a specific email or there is a need to put an appropriate “Out of Office” message on the account. Such cases would require the signature of that member’s Group Support Manager on the RIPA form after appropriate consultation

with the relevant Group Whip. There has been one occasion where such intervention has been necessary within the last six months and this was in order to provide alternative contact details for people seeking assistance following the death of a Councillor.

3.20 Actions on an email account which are covered by the RIPA as described above are undertaken only by specific email administrators. The system administrators have full control over the email system within both the Lotus Notes and the new Outlook/Exchange environments.

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 The projects and services included in this report are designed to provide members with technical support using established best practice practices and processes.

7.0 Recommendations

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

APPENDIX A

LEEDS CITY COUNCIL

MEMBERS E-MAIL CODE OF PRACTICE

1 INTRODUCTION

1.1 The purpose of this Code of Practice is to make sure the Council's e-mail facilities are used properly by all users.

1.2 E-mail facilities are provided to Members to enable them, or assist them in carrying out their duties as elected representatives. However, some incidental personal use by Members is allowed (see below). E-mail facilities are provided to Members primarily for Council business, to help them carry out their duties as elected representatives. However, by agreement the facilities can also be used by Members for other secondary personal uses. All users are personally responsible for complying with the rules for email use in this Code of Practice, and for making sure they use e-mail in a way which is compatible with the Council's Core Values.

1.3 E-mail correspondence is subject to the same internal Council rules, policies and procedures as other Council communications. It also has the same legal status as other communications, so it could create a contract, or someone could claim they were being harassed by email.

1.4 E-mail correspondence is subject to legal restrictions, just like other communications. Information must not be sent by e-mail, where this would break data protection or human rights rules about not disclosing personal data or private information.

1.5 All users must be vigilant about making sure their own e-mail account and the Council's systems generally are kept secure, and must comply with the rules about the security of the Council's systems.

1.6 Breaches of the rules for e-mail use in this Code of Practice by Members may result in allegations of misconduct to the Monitoring Officer. Where criminal conduct may have occurred, breaches may also be reported to the Police. E-mail users who breach the data protection rules could face prosecution.

2. RULES FOR E-MAIL USE

2.1 Members use e-mail to help them carry out their duties as elected representatives, subject to incidental personal use (see below). Where an Elected Member has entered into an agreement to make other secondary private use of a computer, all such use must also be in accordance with the following rules.

2.2 Generally, users must make sure their e-mail correspondence conforms to the Council's rules, policies and procedures.

2.3 In particular, users must not engage in any e-mail correspondence which would constitute a breach of:

- The Disciplinary Rules, Code of Conduct, and Disciplinary Procedures.
- Policies relating to dignity at Work.
- The Equalities Policies.
- The Members Code of Conduct.

2.4 Users must not create and/or send messages and/or attachments to messages that are, or which reasonably could be regarded as being:

- obscene
- pornographic
- indecent
- of a sexual nature
- violent
- a serious attack on someone's reputation
- racist, sexist or otherwise discriminatory or harassing
- threatening or intimidating
- encouraging or supporting racism, sexism, violence, drug taking or gambling

Where Elected Members have to send email or attachments with this content, as part of their duties as elected representatives, they must have prior authorisation from the Chief Democratic Services Officer (or nominee).

2.5 Users must not use e-mail to disclose information, where this would break data protection or human rights rules.

2.6 Users must not send non-Council related advertisements, chain letters other unsolicited non business related email.

2.7 Users must not create or exchange information, logos etc. which belong to someone else, in contravention of copyright or other intellectual property laws.

2.8 Users must not commit the Council to any contract or agreement other than in compliance with the Council's Contracts Procedure Rules, and Financial Procedure Rules.

2.9 Users must not (unless authorised to do so as part of proper proxy arrangements, and/or where they have the consent of the other e-mail user):

- give their passwords to others.
- read e-mail in, or send email from another e-mail user's account.
- alter e-mail or attachments which they have received, or which are in another email user's account,
- add or delete attachments to e-mail which they have received, or which are in another e-mail user's account,

2.10 Incidental e-mail correspondence (i.e. which is personal, political or business in nature), is allowed as long as it does not have an adverse effect on service levels. All such e-mail by Members, must still comply with the rules for e-mail use in this Code of Practice, and will still be subject to monitoring. It should also be noted that private, business and political emails may be associated with the Council by the recipient in that any email issued identifies the Member @leeds.gov.uk.

2.11 E-mail correspondence on a matter which becomes, or might become subject to court action should be kept (and not deleted from e-mail systems), because it might need to be disclosed in court. If a matter is subject to court action, internal e-mail correspondence should be avoided.

2.12 E-mail correspondence on a matter which is the subject of a request for information under the Freedom of Information Act 2000 must not be deleted until after the request has been dealt with, and any complaint or application to the Information Commissioner has been determined.