

AGENDA ITEM 6

POLICY, FINANCE AND ADMINISTRATION

30 SEPTEMBER 2014

REPORT OF HEAD OF CENTRAL SERVICES

ICT POLICIES

1.0 PURPOSE OF REPORT

1.1 The purpose of this report is to present a number of Information and Communication Technology (ICT) Policies that have been reviewed and updated following recommendations made by Internal Audit.

2.0 RECOMMENDATIONS

2.1 It is recommended that The Council:

A – consider and approve the ICT Policies (Appendices 1 – 18);

B – consider and approve a change in Delegation to allow :

- the Head of Central Services to approve technical policies and minor changes to all policies;
- the Head of Central Services in consultation with the Management Team to approve procedural and advisory policies; and
- Policy, Finance & Administration Committee to approve user policies.

3.0 KEY ISSUES

3.1 ICT Policy Review

In March 2014 Internal Audit undertook a review of the ICT Policies. As a result of that Audit it was recommended that the ICT Policies were reviewed and updated. This report summarises the changes made to the ICT Policies, and subject to agreement, will be submitted to The council for sign off. The updated policies are shown below.

3.2

| Ref | Description | Source | Type |
|------|---------------------|--------|------------|
| 001d | User Guide | MBC | Advisory |
| 001e | Personal Use | MBC | Advisory |
| 002 | Account Passwords | IT | Technical |
| 004 | Procurement | IT | Procedural |
| 007 | Change | IT | Procedural |
| 008a | Network Cables | MBC | Technical |
| 009 | Disposal | IT | Procedural |
| 011 | Exchange Management | IT | Technical |
| 017 | Replacement | IT | Procedural |

AGENDA ITEM 6

| | | | |
|------|---------------------------|-----|------------|
| 018 | IT Security | IT | User |
| 018a | Personal and Confidential | MBC | Advisory |
| 019 | Security Incident | IT | Procedural |
| 022 | Patching | IT | Technical |
| 024a | Remote Access | MBC | Technical |
| 027 | Third Party | IT | Procedural |
| 041 | Cloud | IT | Advisory |
| 043 | PSN | IT | User |

- 3.3 The table above lists the Policies that have been reviewed and have been categorised as follows :

Source

MBC – are reviewed MBC Policies that have had only marginal changes applied.

IT – are new Policies that have been introduced or completely rewritten

Type

Advice – This documents provide advice / guidance to users

User – these policies require staff to confirm understanding and can result in disciplinary action

Technical – are technical IT documents concerning the setup of systems

Procedure – these are procedural documents stating how activities will be delivered.

- 3.4 The primary changes are in 011 Exchange Management, 018 IT/IS Security and 024a Remote Access.
- 3.5 Two changes have been made to the Exchange Management Policy. The first introduces a limit to the mailbox size and the second removes the Auto Forward feature.
- 3.6 The Exchange Mailbox size has been limited to 500M for standard users and 1G for Senior Managers. This will require the introduction of email archiving processes although the aim is to efficiently manage expensive online storage, rather than clutter it up with several years of old emails. These limits will be phased in to ensure that colleagues are not faced with an immediate impact upon their working practices.
- 3.7 Leicestershire County Council have recently reviewed their ICT Policy and stopped the use of 'Auto Forward' from email accounts. In consultation with LCC, MBC will be adopting the same principle. This rule is being adopted to ensure that appropriate measures are in place to protect the security and integrity of personal and sensitive information. Emails can still be forwarded, although they must be done manually. The implication of this rule (for Members, Partners and Staff) will be that users will need to log on to the MBC network to see any emails i.e. using the Vasco token and network login.

AGENDA ITEM 6

3.8 The IS/IT Security Policy has been rewritten and now represents a summary of the key Information Technology and Information Security Policies. The contents are not new, however, the document brings together the information in one place.

3.9 Policy 024a Remote Access Policy has been largely unchanged. Although, the clause stating that Council devices should not be taken outside the UK has been amended to allow Mobile Telephones to be taken outside the UK with appropriate safeguards.

3.10 Change to Delegated Powers

This Policy review has highlighted the overly bureaucratic process required to update the Authorities ICT Policies which under the current delegation requires full council approval. The majority of the Policies are dictated by best practice and Government Security requirements; their impact is primarily operational and as such could be approved by Senior Officers. This is not to remove Member engagement, but to delegate technical, procedural and advisory policies to officers whilst leaving the key user policies for Committee Approval. The following outlines proposed revisions to the ICT Policy approval process for members consideration:

- the Head of Central Services to approve technical policies and minor changes to all policies;
- the Head of Central Services in consultation with Management Team to approve procedural and advisory policies; and
- Policy, Finance & Administration Committee to approve user policies.

4.0 POLICY AND CORPORATE IMPLICATIONS

4.1 The ongoing commitment to the Partnership aims to improve the running of ICT Services through a new contract. It aims to provide a more efficient service by working together with neighbouring Authority's. These aims are consistent with the corporate aim to be a well run Council and to provide good services that are value for money.

5.0 FINANCIAL AND OTHER RESOURCE IMPLICATIONS

5.1 The proposals have no direct financial or resource implications, although the proposed revision to the ICT Policy approval process will be more efficient.

6.0 LEGAL IMPLICATIONS/POWERS

6.1 The adoption of the revised ICT Policies, including the amended auto-forwarding procedure, will help to ensure continuing compliance with the requirements of the Data Protection Act 1998, and particularly with the requirement in Data Protection Principle 7, that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

AGENDA ITEM 6

7.0 COMMUNITY SAFETY

7.1 The proposals have no direct impact upon Community Safety.

8.0 EQUALITIES

8.1 An equalities impact assessment was undertaken and raised no areas of concern.

9.0 RISKS

9.1 This report enables the Committee to approve ICT policies for recommendation and does not place the Council at risk. The changes to the approval process still require Members to approve key user policies and again does not place the Council at risk.

9.2 Out of date ICT policies and procedures can result in regulatory issues and limit the ability to address breaches. As such the approval of these policies reduces this risk. The main risk that the policies aim to mitigate are security breaches and the Central Services service plan shows the residual risk to the council to be as set out in the table below:

Probability



| | | | | |
|---------------------------|-----------------------|----------------------|----------------|------------------------|
| Very High A | | | | |
| High B | | | | |
| Significant C | | 1 | | |
| Low D | | | 2 | |
| Very Low E | | | | |
| Almost Impossible F | | | | |
| | IV Neg- ligible | III Marg- inal | II Critical | I Catast- rophic |

→
Impact

| Risk No. | Description |
|----------|----------------------------|
| 1 | Security breach - internal |
| 2 | Security breach - external |

10.0 CLIMATE CHANGE

10.1 These proposals have no effect on climate change.

AGENDA ITEM 6

11.0 CONSULTATION

11.1 Management Team, Programme Board, Joint Staff Working Group and the Leader of the Council have been consulted on these changes. Liaison is still being undertaken with LCC to potentially allow the auto-forward of e-mails to LCC accounts and the committee will be updated verbally on the evening should this be possible.

12.0 WARDS AFFECTED

12.1 Wards are not directly affected by these projects but all people living in the Borough will benefit from more efficient delivery of IT.

Contact Officer Dawn Garton/ Paul Langham

Date 4 September 2014

Appendices

- Appendix A – User Guidance
- Appendix B - Personal Use
- Appendix C - Account Password Settings
- Appendix D - Procurement and Asset Management Policy
- Appendix E – Change and Incident Management Policy
- Appendix F – Network Cable Colours
- Appendix G – Disposal
- Appendix H – Exchange Mailbox
- Appendix I - Replacement
- Appendix J – ICT Security Policy
- Appendix K – Personal and Confidential Data
- Appendix L - ICT Security Incident Procedure
- Appendix M - Patch Management
- Appendix N – Remote Access
- Appendix O – Third Party Support
- Appendix P – Cloud Storage Policy
- Appendix Q – PSN AUP Policy