Derby City Council

Personnel Committee
4 September 2018

ITEM 12

Report of the Strategic Director of Corporate Resources

Information Security and IT Acceptable Use Policy

SUMMARY

1.1	Information Security covers the safekeeping of all forms of information, electronic and non-electronic, to protect its confidentiality, integrity and availability.
1.2	This report seeks endorsement to a refreshed Information Security and IT Acceptable Use Policy.
1.3	The Information Security and IT Acceptable Use Policy is a consolidation of several existing policies. It is not the creation of new policy. There are no material changes to already ratified policy within the Council.
1.4	The policy will be promoted through the Keeping In Touch and Managers' Briefing cascade.

RECOMMENDATIONS

2.1	That the Personnel Committee formally agrees and endorses the revised policy.

REASONS FOR RECOMMENDATIONS

3.1	We are required to maintain a minimum level of Information Security to maintain our legal and contractual obligations. Well published, approved and regularly refreshed, policies and standards of information security are necessary to define the parameters in which we operate. By understanding and implementing our responsibilities we can make sure our citizens have trust and confidence in the way they can access our systems and the way we manage, store, share and use our information assets.

SUPPORTING INFORMATION

4.1	The policy incorporates the evaluation, amalgamation and assimilation of eight policies comprising 40 pages in to one policy of 25 pages. It is explained in simpler terms and items are removed or amended to reduce the 'technical jargon' that staff do not want or need to know. This allows for a single point of reference for staff to the majority of Information Security and IT Acceptable Use standards.

	The policies being replaced by this policy are: • Information Security Policy v9.1 • Laptop, Desktop and Tablet Device Security Policy • Email, Internet Security and Monitoring Policy • Remote and Mobile Computing Policy • Email and Internet User Policy • Internet File Sharing and Collaboration Sites Policy • Malware Prevention policy • Network User Policy
4.2	The refreshed policy has been subjected to extensive consultation within the Council and agreed by the Council's Information Governance Board.
4.1	The refreshed policy is promoted in conjunction with the new GDPR and Cyber Security e-learning. InTouch and iDerby bulletins are used to highlight the policy, along with directed communications to Managers, for dissemination. All staff are required to complete a review of the policy as part of corporate induction and should complete a review annually. The policy is readily available in the Governance pages of iDerby for staff to access. The policy is also embedded into the information breach process: Where human error is a factor, individuals and teams are requested to complete a review of the policy on the training portal.

OTHER OPTIONS CONSIDERED

5.1	Not applicable.

This report has been approved by the following officers:

Legal officer **Financial officer** **Human Resources officer** **Estates/Property officer** **Service Director(s)** **Other(s)**	Not applicable Not applicable

For more information contact: **Background papers:** **List of appendices:**	Andy Preston 01332 643117 andy.preston@derby.gov.uk None Appendix 1 – Implications Appendix 2 – Information Security and IT Acceptable Use Policy

Appendix 1

IMPLICATIONS

Financial and Value for Money

1.1 There are no direct financial implications, however the Information Commissioners Office could award significant fines to Council's who do not properly protect the personal information that they manage.

Legal

2.1 The Council has obligations under information legislation, including the Data Protection Act 2018, to protect its information assets.

Personnel

3.1 Every person is responsible and accountable for putting into practice these policies, standards and procedures.

3.2 The policy highlights a level of responsibility for line managers to ensure all persons have authorised use of the Council's IT systems and that they are aware of the management of non-electronic information.

IT

4.1 The policy defines the standards that users of Council's IT systems must abide by.

Equalities Impact

5.1 None

Health and Safety

6.1 None

Environmental Sustainability

7.1 None

Property and Asset Management

8.1 None

Risk Management

9.1 A data breach must be reported for it to be recorded and investigated.