Derby City Council

Corporate Joint Committee
1 December 2016

ITEM 5

Report of the Director of Governance and Monitoring Officer

Software Licensing Policy

SUMMARY

1.1 This Policy sets out the rules to ensure we comply both with mandatory compliance regulations including UK and European Union laws and that we comply with contracted licence terms.

1.2 The report seeks to introduce this revised and updated Policy that aims to make staff and Elected Members aware of their responsibilities and the things they should – or should not – do to work safely and securely and that they only use licenced software.

RECOMMENDATIONS

2.1 The Policy will avoid the risk of civil or criminal action for breach of contract, software misuse or breach of copyright/intellectual property rights or of noncompliance with security regulations for the Council.

2.2 To authorise the adoption and implementation of the Software Licensing Policy with immediate effect.

2.3 To note that promotion of this Policy will be cascaded widely across to raise awareness with Elected Members and Staff

2.4 To authorise the Director of Governance to make minor amendments to the Policy which may be needed in the future such as amend details of named officers however any changes which alter the nature or intent of the policy will require the approval of Personnel Committee

REASONS FOR RECOMMENDATIONS

3.1 It is important that Derby's citizens are able to trust the Council to act appropriately when obtaining, holding and sharing information when using the authority's facilities. It is also important that information owned by other organisations which is made available to the Council under secondary disclosure agreements is treated appropriately. 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.

3.2 The Policy is explained in simpler terms and the document has been shortened and items removed or amended to reduce the ‘technical jargon’ that staff do not want or need to know.

3.3 The Information Governance Board must review all policies and authorise all changes. They would recommend formal ratification of policies where the nature or intent had been amended. If committee approval is not required the Policy would be published and the committee informed at the next meeting.

SUPPORTING INFORMATION

4.1 Maintaining compliance with third party Codes of Connection for example the Public Services Network, a programme designed by the UK Government to create one ICT network for all UK public sector organisations.

4.2 Applying the International Standard ISO/IEC 27001:2013 standard specification for Information Security Management which defines Information Security as protecting three aspects of information:

- *confidentiality* - making sure that information is accessible only to those authorised to have access
- *integrity* - safeguarding the accuracy and completeness of information and processing methods
- *availability* - making sure that authorised users have access to information and associated resources when required.

4.3 The Business Software Alliance, an international regulatory body protecting against software piracy, can fine businesses that contravene software licensing laws and even incentivise employees to act as whistle-blowers.

OTHER OPTIONS CONSIDERED

5.1 Software licensing must comply both with mandatory compliance regulations including UK and European Union laws and we must comply with contracted licence terms. We are all required to maintain a minimum level of Information Security to maintain our legal and contractual obligations. Defined and approved policies and standards of information security must be implemented.

5.2 Failure to issue a Policy increases the risks which, should we be found in breach of software licencing, could lead to action against the Council for not having relevant controls and a clear Policy.

This report has been approved by the following officers:

Legal officer	Janie Berry - Director of Governance and Monitoring Officer
Financial officer	Not applicable
Human Resources officer	Liz Moore - Strategic HR Business Partner
Estates/Property officer	Not applicable
Service Director(s)	Nick O'Reilly – Director of Digital Services
Other(s)	Richard Boneham – Head of Governance & Assurance

For more information contact:	Angela Gregson 01332 642670 angela.gregson@derby.gov.uk
Background papers:	None
List of appendices:	Appendix 1 – Implications Appendix 2 - Organisation and Governance: Remote and Mobile Computing Policy v2.0

IMPLICATIONS

Financial and Value for Money

1.1 There are no direct financial implications unless a breach of contracted software licence terms by the Council occurred which resulted in a fine.

Legal

2.1 There are no direct legal implications unless a breach of software contracted licence terms by the Council occurred.

Personnel

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

3.2 The Policy will apply to all persons (staff and Elected Members) having legitimate access to Council systems and data. It has gone through the agreed consultation procedures with the Trade Unions.

IT

4.1 The IT implications are covered in the body of the report.

Equalities Impact

5.1 We have done one equality impact assessment, which is attached, covering the suite of Information Security Policies and this highlights the positive impact information security has on people with protected characteristics.

Health and Safety

6.1 None

Environmental Sustainability

7.1 None

Property and Asset Management

8.1 None

Risk Management

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

Corporate objectives and priorities for change

10.1 The Council aims to be a leading digital organisation, with a modern way of working that facilitates staff, customers and partners. It endeavours to try and ensure that the computer network is safe and secure for staff and its customers.

10.2 The Council's objective is to reduce the risk of information security incidents and be able to demonstrate to the citizens and businesses of Derby that we collect, handle and store their information securely.

Appendix 2

Information Systems Governance:

Software Licensing Policy

Document owner	Information Systems Client Team Manager
Document author	Nick O’Reilly
Document date	July 2016
Version	5.0 – Draft for review
Document classification	Official
Document distribution	Published via the Council Intranet
Next review date	July 2017

Version Control

To make sure you are using the current version of this policy please check on iDerby or contact Information Governance when using printed copies.

Version Number	Date	Author	Reason for Version
4.0	June 2009	Alison Moss	
5.0	July 2016	Nick O’Reilly	Replace old and obsolete policy

Document Approval

Job Role	Approvers Name	Date Approved
Director of Digital Services	Nick O’Reilly	26 July 2016
Information Governance Board	Richard Boneham	26 July 2016
Conditions of Service Working Party	Janie Berry	
Personnel Committee		
Corporate Joint Committee		

Please tell us if you need this in large print, on audio tape, computer disc or in Braille.
You can contact Ann Webster on 64 3722, Minicom: 01332 64 0666 or Text Relay: 18001 01332 643722

Contents

1. Introduction………………………………………………………………….. 8
2. Scope………………………………………………………………………… 9
3. Software Installed on Servers or Hosted centrally……………………………. 9
4. Software Installed on End User Devices………………………………………. 9
5. Software and Apps on Mobile phones…………………………………………. 10
6. “Freeware” or “Shareware”……………………………………………………. 10
7. License Types, Per Seat, Per User, Concurrent……………………………… 10
8. Use by or Transfer to 3rd Parties……………………………………………….. 11
9. Software Auditing……………………………………………………………… 11
10. Security, Compliance and Integrity…………………………………………….. 12
11. Responsibilities and Accountabilities………………………………………….. 12
12. Compliance with theSoftware Licensing Policy………………………………. 12
13. Other Relevant Policies, Standards and Procedures………………..……… 13
14. Contact Details………………………………………………………………… 13

1. Introduction

The reason we need a software licensing policy is to ensure we comply both with mandatory compliance regulations including UK and European Union laws and that we comply with contracted licence terms.

This will avoid risk of civil or criminal action for breach of contract, software misuse or breach of copyright/intellectual property rights or of noncompliance with security regulations.

2. Scope

2.1 This Policy applies to ALL software used by all employees of the Council, elected members, contractors, agents, partners and temporary staff who have authorised access to Council IT systems who can work remotely and use mobile computing equipment. This includes staff that access Council email from smart-phones.

2.2 It applies to all software installed on the Council's computers and any software installed by the Council with the employees or member's consent to support Bring/Use your own device.

2.3 Only licensed software can be installed and used, on no account should unlicensed software be installed and used.

3. Software Installed on Servers or Hosted centrally

3.1 Most business software will be installed on servers and/or hosted centrally or under contract with a remote data centre. Only nominated system administrators will be physically allowed to install such software.

3.2 Where new software is ordered and needs installing the IS department will need to manage this process and will require the business service to confirm they have the required licences. If the software has been purchased using the IS procurement process this will be managed as part of the procurement to installation process.

3.3 It is the responsibility of the business owner to ensure a copy of the software licence terms is lodged with the master contract and for providing any software keys to the IS department.

3.4 The IS department when provided with information will keep a record for each software of the product licence key, the licence type and the maximum number of per seat and/or concurrent users permitted.

4. Software Installed on End User Devices

4.1 Where software has to be installed on end user devices, by which we mean desktop, laptop or tablet computers then wherever possible this will also be restricted to nominated system administrators. If that is not possible a full record of each installation needs to be made with approval from the IS department prior to installation.

4.2 The business owner remains responsible for the contract documents and the master licence copy but must forward all technical details, installation guides and licence product keys to the IS department.

4.3 If possible such software will be deployed using software management tools and not locally on each computer; this increases controls and avoids licence noncompliance.

4.4 The Council endeavours to prevent the downloading of software (executable files and scripts) to such devices as to do so can unwittingly introduce malware or viruses. Users must not try to download applications for software even if prompted to do so by a website or pop up notification. If such software is required for the business it needs to be authorised using the IS approval process.

4.5 The asset records for such software installations will be maintained using software asset management tools that detect and monitor the presence of software.

4.6 No non-Council approved software or internet available apps can be installed or downloaded; if such is found this will lead to disciplinary investigation.

5. Software and Apps on Mobile phones

5.1 The Council accepts that mobile phones encourage the use of apps which download software to the phone device. The Council will not bar employees form doing this to their work provided phone but notes each user is responsible for ensuring they read and understand the licence terms that apply.

5.2 On no account should Council data be entered into such software or apps because the data may be stored outside of the European Union which could breach the Data Protection Act and would breach our compliance obligations for security.

5.3 The same apps should not be downloaded or installed to any Council provided laptop or tablet devices because there is an increased risk of network intrusion and malware infection. If such apps are required for business use these need to be installed in accordance with the end user device installation procedures.

6. “Freeware” or “Shareware”

6.1 Freeware and Shareware are terms used to describe software that appears to be or is free to use. Just because it is free does not mean there are not software licensing obligations. Often there are obligations to allow access to the supplier to its use, access to data or even requirements after a period of free use to have a period of use that incurs charges.

6.2 Most Freeware and Shareware also have terms that prevent their use or distribution for profit or to other users; requiring each user to licence with the Freeware/Shareware provider directly. Just because it is free does not mean it does not have terms of use that are legally enforceable.

7. License Types, Per Seat, Per User, Concurrent

7.1 We must only install or use the permitted number of copies of any software and only make back-up copies as we are legally entitled to.

7.2 If a licence is per seat it means it can only be installed on the stated number of devices; this can deter flexible working where a user may want the software on more than one device.

7.3 If a licence is per user it allows the same user to access the software from any device, the Microsoft software is moving to per user allowing greater flexibility and opening up bring/use your own device opportunities; other software may follow suit.

7.4 Concurrent user means we can install software for use across the organisation but limited to a number of concurrent users; if one more user tries to access they will receive a message saying all copies are in use.

7.5 It is important that the business considers carefully how it uses software and chooses the best licence option (If a supplier offers choice).

8. Use by or Transfer to 3rd Parties

8.1 If your service may need non staff to use the software this needs to be checked carefully before entering into the software licence. Most software vendors will allow use by staff and agency workers, and some will extend to partners and volunteers provided the work is for our purposes. However some will explicitly not allow use by any 3rd party.

8.2 If the Council is transferring services to 3rd parties be this under partnership agreements, community volunteer arrangements, as formal outsourcing or to Charitable trusts then the software licensing terms need to be checked. **DO NOT ASSUME THIS IS PERMITTED OR IT IS FREE!** This has proven to be an issue when the Museums Trust was established.

8.3 If you are not sure you need to check with both the Information systems (IS) and the Legal Department before allowing any 3rd party use, and certainly before transferring any software asset to a 3rd party.

9. Software Auditing

9.1 The IS department will manage all software and will prepare and agree upgrade schedules required to maintain compliance.

9.2 The IS department will also implement and maintain a software auditing tool that can detect and check software installed; but with limited resources such checks will be sporadic and in response to suspected abuse or after an alert that un-authorised software has been installed or detected. The IS department will also implement and maintain a software auditing tool that can detect and check software installed; these checks will be annual and additionally in response to suspected abuse or after an alert that un-authorised software has been installed or detected.

9.3 Other parties including internal and external audit and software suppliers (who have rights to inspect and audit in their contract terms) may also undertake audits and any unlicensed or under-licensed software found may lead to both financial penalties and disciplinary investigation.

10. Security, Compliance and Integrity

10.1 To install non approved and/or unlicensed software is a breach of the Council's mandatory security, compliance and integrity obligations; and as such there is zero tolerance imposed upon the Council by compliance authorities.

10.2 Any breach of this Software Policy will therefore result in the devices upon which it has been found being placed into quarantine and the user accounts suspended pending investigation. If the investigation confirms that non-approved and/or unlicensed software has been installed it will be removed and disciplinary action may follow.

10.3 If such software has been installed in contravention of these rules then the person responsible could also face civil or criminal action either from the software supplier or from other parties whose data may have been put at risk due to unauthorised software (be this hidden malware or software that has embedded code that accesses or stores data in contravention of UK and European laws.).

11. Responsibilities and Accountabilities

11.1 The Head of Governance & Assurance has responsibility for defining the Council's information security policies, standards and procedures which are approved by the Information Governance Board. Every employee, and in particular line managers, is responsible and accountable for putting into practice these policies, standards and procedures.

11.2 ***Information Security is not an option.*** We are all required to keep a minimum level of security to meet our legal and contractual obligations; and data sharing protocols with our partners.

12. Compliance with the Software Licensing Policy

12.1 The Head of Governance & Assurance is responsible for monitoring compliance with this policy.

12.2 If employees knowingly do not comply with Council policies, procedures or guidelines, the Council may take appropriate action in accordance with the Employee Code of Conduct.

12.3 Use by Councillors must at all times be in accordance with the standards and Code of Conduct set for councillors. If it is reported that there has been a breach of the Code of Conduct then in accordance with the procedures for councillor's the matter will be referred to the Monitoring Officer.

13. Other Relevant Policies, Standards and Procedures

These can be found on iDerby or contact the Information Governance team.

14. Contact Details

Please contact the Council’s Head of Governance & Assurance or anyone in the Information Governance team with enquiries about this or any other referenced policy, procedure or law.

Email to:	information.governance@derby.gov.uk
Telephone:	01332 640763