Derby City Council

Personnel Committee
7 July 2016

ITEM 7

Report of the Director of Governance and Monitoring Officer

Internet File Sharing and Collaboration Sites Policy

SUMMARY

1.1 This policy is to explain the controls we will apply in respect of registration and/or use of internet file sharing and other collaboration tools.

1.2 The report seeks to introduce a new policy that aims to make staff aware of their responsibilities and the things they should – or should not – do to ensure we comply with the Data Protection Act and with associated information sharing compliance regulations.

RECOMMENDATIONS

2.1 The policy will raise awareness on the security of sharing data using internet file sharing and other collaboration tools as the use of these sites could lead to a serious breach of data security.

2.2 To adopt the new policy that was agreed with the Trade Unions at CoSWP on 10 June 2016.

2.3 To promote this new policy through the In Touch and Manager's Briefing cascade process.

2.4 To agree that future changes to the policy, for example, to amend named officers and/or to bring these up to date do not need formal ratification. Any changes that alter the nature or intent of the policy, for example, changing the policy to allow use of an agreed internet file sharing utility would need ratification.

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 simple terms and the document has been written without

'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 The use of any file sharing or internet collaboration tools must comply with the following regulations:

- Prevailing United Kingdom and European Union Data Protection Regulations and associated guidance issued by the Information Commissioners office.
- Prevailing NHS and Social care information sharing regulations including the NHS Information Governance Toolkit and the Caldicott guidelines.
- Prevailing Pubic Sector Network and inter-government data sharing regulations.
- Prevailing Payment Card Industry regulations.
- The Common Law Duty of Confidentiality
- Other relevant regulations that may be applicable to one or more Council services

4.3 Applying the seventh principle of the Data Protection Act:

> 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.

OTHER OPTIONS CONSIDERED

5.1 Information security is not an option. 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 a data breach occur, 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	Diane Sturdy
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: Internet File Sharing and Collaboration Sites Appendix 3 – Equality Impact Assessment, see item 5 on the agenda

IMPLICATIONS

Financial and Value for Money

1.1 There are no direct financial implications unless a data breach caused the Council to be unable to fulfil its role and/or resulted in a fine from the ICO.

Legal

2.1 There are no direct legal implications unless a data breach caused the Council to be accountable to the ICO.

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 having legitimate access to Council systems and data. It has gone through the agreed consultation procedures with the Trade Unions.

IT

4.1 The data may be hosted on servers outside of the European Union and in territories without equivalent data protection regulations.

4.2 Data uploaded to such sites is not always fully encrypted and may be subject to unauthorised access.

4.3 We cannot audit or control data once uploaded, and therefore cannot ensure unauthorised access does not occur, or if it does cannot trace the access and take mitigation action.

4.4 We cannot control and remove access from former employees/agency staff when they leave and thus they may still have access to confidential documents.

4.5 Many of the providers of such sites include in their terms and conditions either transfer of ownership of the uploaded documents and images or a right for the site to share them without consent of the owner. They also often transfer the jurisdiction for any disputes outside of the UK and European Union.

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.

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

Organisation and Governance:
Internet File Sharing and Collaboration Sites

Document owner	Senior Information Risk Officer (SIRO)
Document author	Nick O'Reilly
Document date	May 2016
Version	1.0 First Draft
Document classification	Official
Document distribution	Published via the Council Intranet
Next review date	01 June 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
1.0	June 2016	Nick O'Reilly	New

Document Approval

Job Role	Approvers Name	Date Approved
Director of Digital Services	Nick O'Reilly	24/5/16
Information Governance Board	Head of Governance & Assurance - Richard Boneham	24/5/16
CoSWP	Director of Governance & Monitoring Officer - Janie Berry	10/6/16
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

The purpose of this policy is to explain the controls we will apply in respect of registration and/or use of internet file sharing and other collaboration controls.

The reason we need such a policy and controls is to ensure we comply with the Data Protection Act and with associated information sharing compliance regulations.

This policy applies to all employees of the Council, elected members, contractors, agents, partners and temporary staff who have authorised access to Council IT systems.

2. Compliance with Regulations

The use of any file sharing or internet collaboration tools must comply with the following regulations:

- Prevailing United Kingdom and European Union Data Protection Regulations and associated guidance issued by the Information Commissioners office.
- Prevailing NHS and Social care information sharing regulations including the NHS Information Governance Toolkit and the Caldicott guidelines.
- Prevailing Pubic Sector Network and inter-government data sharing regulations.

- Prevailing Payment Card Industry regulations.
- The Common Law Duty of Confidentiality

- Other relevant regulations that may be applicable to one or more Council services.

3. Definition of an Internet File Sharing/Collaboration sites.

The Council defines an internet file sharing or collaboration tool as a tool that allows users to connect with each other and to upload or download files from an internet location.

Examples include Dropbox, Google- drive, Microsoft One Drive, but there are many other such tools.

4. Why These Sites Are Not Allowed

4.1 The use of such sites poses a number of risks that could lead to a serious breach of data security, these include:

- The data may be hosted on servers outside of the European Union and in territories without equivalent data protection regulations.
- Data uploaded to such sites is not always fully encrypted and may be subject to unauthorised access.
- We cannot audit or control data once uploaded, and therefore cannot ensure unauthorised access does not occur, or if it does cannot trace the access and take mitigation action.
- We cannot control and remove access from former employees/agency staff when they leave and thus they may still have access to confidential documents.
- Many of the providers of such sites include in their terms and conditions either transfer of ownership of the uploaded documents and images or a right for the site to share them without consent of the owner. They also often transfer the jurisdiction for any disputes outside of the UK and European Union.

4.2 We are exploring the possibility of an internet file sharing utility that can meet the respective data protection and information sharing regulations and that can be managed in terms of audit trails, access security and user account management but until we can establish such we have no option to prohibit the use of such internet file sharing/collaboration sites.

5. Registration with Such Sites with your Council Email

5.1 For the avoidance of doubt **no** Council employee, contractor or councillor is allowed to register for internet file sharing and collaboration sites using their derby.gov.uk email. Any employee doing so may face disciplinary action.

5.2 If you can justify a valid need to do this, then on approval of a business case that explains why this is needed and how we can address the security requirements permission may be given by the Information Governance team and/or the Council's Senior Information Risk Owner. A register of such exceptions to the otherwise total ban on such sites will be held centrally.

6. Using a Personal Registration for Council Business

6.1 We cannot prevent staff registering for such sites with their own, non-council, email. However, uploading Council data to such sites using a personally registered email account is a breach of Council policy and may lead to disciplinary action.

6.2 Employees, agency staff, and Councillors all have obligations to access, store and manage Council provided information in accordance with both prevailing regulations (see section 2 above); and in accordance with Council policies and procedures.

6.3 Even if the files uploaded do not contain personal data all files and data held by the Council for Council business remain the property of the Council and copying these to internet file sharing/collaboration sites may put at risk Council data**.**

7. Compliance with the Code of Conduct

7.1 The Head of Governance & Assurance is responsible for monitoring compliance with this policy and will advise the Council's Senior Information Risk Officer (SIRO) and Chief Officers both periodically and following major incidents.

7.2 If employees, agency staff or other 3rd parties granted access to the network knowingly do not comply with Council policies, procedures or guidelines, the Council may take appropriate action in accordance with the Employee Code of Conduct.

7.3 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.

8. Other Relevant Policies

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

9. 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