



Derby City Council

Personnel Committee
7 July 2016

Report of the Director of Governance and
Monitoring Officer

ITEM 6

Freedom of Information (FOI) Policy (Internal)

SUMMARY

- 1.1 This policy aims to ensure individuals and organisations have access to information held by the Council in order to promote greater openness, providing increased transparency of decision making and to build public trust and confidence.
- 1.2 The report seeks to introduce a new policy that aims to make staff aware of their responsibilities to ensure that the Council complies with the Freedom of Information (FOI) Act 2000.
- 1.3 This policy does not cover Subject Access Requests (SAR). These are requests about information relating to the requestor or about an individual the requestor is authorised to act on behalf of and should be processed in accordance with the Data Protection Act 1998 (DPA).

RECOMMENDATIONS

- 2.1 This policy covers all requests for information except requests from individuals for their own personal data and 'business as usual' requests. A 'business as usual' request is a request for information or services that a service area would expect to receive in its normal day to day operation. Any request that indicates it is an FOI request cannot be treated as 'business as usual'.
- 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, if there are changes to the Freedom of Information (FOI) Act 2000 that change the way the Council has to provide information including timescales for responding.

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 Freedom of Information (FOI) Act 2000 provides individuals and organisations with the right to request information held by, or on behalf, of the Council. As a local authority we must comply with the Act. The Act applies to all recorded information held by the Council or by someone else on behalf of the Council.
- 3.3 The policy is explained in simple terms and details to staff how to action requests they receive and the process that the FOI team will invoke to ensure the Council responds to requests within the 20 working day time limit.
- 3.4 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 Council is under a legal duty to protect personal data as required by the Data Protection Act 1998 (DPA). The Council will carefully consider its responsibilities under the DPA before disclosing personal data about living individuals, including current and former officers, members, and users of its services.

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 Financial officer Human Resources officer Estates/Property officer Service Director(s) Other(s)	Janie Berry - Director of Governance and Monitoring Officer Not applicable Diane Sturdy Not applicable Nick O'Reilly – Director of Digital Services Richard Boneham – Head of Governance & Assurance
For more information contact: Background papers: List of appendices:	Angela Gregson 01332 642670 angela.gregson@derby.gov.uk None Appendix 1 – Implications Appendix 2 - Organisation and Governance: Remote and Mobile Computing Policy v2.0 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 or a failure to provide information held 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 or a failure to provide information held caused the Council to be accountable to the ICO.
- 2.2 Information must be provided if it is held, unless one or more of the exemptions listed in the legislation applies. An FOI requestor has the right to be told whether the information is held and the right to receive the information, subject to exemptions. This applies regardless of the purpose of the application.

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 IT implications are covered in the body of the report.

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:
Freedom of Information Policy (Internal)**

Document owner	Richard Boneham, Head of Governance & Assurance
Document author and enquiry point	Angela Gregson
Date of document	January 2016
Version	1.0
Document classification	Official
Document distribution	Published via iDerby
Review date of document	December 2016

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.

Date Issued	Version	Status	Reason for change
	1.0	Draft	New policy

Document Approval

Job Role	Approvers Name	Date Approved
Director of Digital Services	Nick O'Reilly	28/1/16
Information Governance Group	Head of Governance and Assurance – Richard Boneham	28/1/16
Personnel Committee		
Corporate Joint Committee		
Conditions of Service Working Party	Director of Governance and Monitoring Officer – Janie Berry	10/6/16



Contents

1. Introduction	9
2. Definition.....	10
3. Freedom of Information Policy	10
4. Responsibilities and Accountabilities	12
5. Compliance with the Freedom of Information Policy	12
6. Other Relevant Policies, Standards and Procedures.....	12
7. Contact Details	12

1. Introduction

- 1.1 The Freedom of Information (FOI) Act 2000 provides individuals and organisations with the right to request information held by, or on behalf, of the Council. As a local authority we must comply with the Act. The Act applies to all recorded information held by the Council or by someone else on behalf of the Council.
- 1.2 This policy applies to all employees of the Council, elected members, contractors, agents, partners and temporary staff working for or on behalf of the Council.
- 1.3 This policy aims to ensure individuals and organisations have access to information held by the Council in order to promote greater openness, providing increased transparency of decision making and to build public trust and confidence.



- 1.4 A request for information does not need to specify itself as an FOI request or refer to the FOI Act for it to be valid.
- 1.5 This policy covers all requests for information except requests from individuals for their own personal data and 'business as usual' requests. A 'business as usual' request is a request for information or services that a service area would expect to receive in its normal day to day operation. Any request that indicates it is an FOI request cannot be treated as 'business as usual'.
- 1.6 Information must be provided if it is held, unless one or more of the exemptions listed in the legislation applies. An FOI requestor has the right to be told whether the information is held and the right to receive the information, subject to exemptions. This applies regardless of the purpose of the application.
- 1.7 This policy does not cover Subject Access Requests (SAR). These are requests about information relating to the requestor or about an individual the requestor is authorised to act on behalf of and should be processed in accordance with the Data Protection Act 1998 (DPA). Please see the Subject Access Requests procedure for more information.

2. Definition

- The Council – Derby City Council
- Should – indicates a recommendation - good practice
- Must – indicates that something has to be done to satisfactory requirements – mandatory
- Must not – indicates that something must not be done - mandatory.

3. Freedom of Information Policy

- 3.1 If you receive a request for information and it cannot be classed as 'business as usual' or it states it is an FOI request you must forward it to the [FOI](#) team without delay. The Council must respond to requests promptly and by the twentieth working day following the date of receipt of the request.
- 3.2 If the FOI team send you or your team a request to provide information you must do so by the deadline given by the team. If you will have problems putting the request together within 18 hours [or 2.5 days] you must tell the [FOI](#) team because we may be able to refuse the request.
- 3.3 To be valid under the FOI Act, requests:
 - Must be in writing;
 - Must clearly describe the information being sought;
 - Can be made by an individual or an organisation;
 - Can be made by letter, fax or email;
 - Must be legible;



- Must contain the name of the applicant and a return postal or email address;
 - Do not have to be written in a special form;
 - Do not need to mention the FOI Act;
 - Do not need to refer to “Freedom of Information”.
- 3.4 If you receive a request that is unclear in what it asks then you must contact the [FOI](#) team promptly who will ask for clarification to enable the request to proceed.
- 3.5 You must not deliberately withhold or dispose of information that is covered by the Act. If you are not happy with some information that has been asked for contact the [FOI](#) team to get advice on exemptions that may apply to the disclosure.
- 3.6 If a request for information is received there are three reasons why the information would not need to be provided. These are:
- the information requested is exempt from disclosure
 - the request is considered a nuisance, unreasonable or repetitive
 - the required fee is not paid within three months.
- 3.7 The Council reserves the right to refuse requests where the cost of providing the information would exceed the statutory cost limit. Where we estimate that complying with a request will take more than 18 hours of officer time, we have a duty to try to assist applicants to make refined requests which are more manageable.
- 3.8 You or your team must not respond directly to the applicant when the FOI team forwards you a request. Your response should be sent to the [FOI](#) team who will package and send the response out. The FOI team will request that you respond within 10 working days; this gives the FOI team time to liaise with the responding service/external parties about exemptions and any other queries raised before the 20 working day response deadline.
- 3.9 You must not delay providing the information to the FOI team – remember we only have 20 working days in which to respond. If the FOI team do not receive a response within 10 working days a chase email will be sent to the service on day 10.
- 3.10 If no response is received after the chase email a breach alert email will be sent on day 15 to the officer responsible for providing response, their Head of Service, Head of Governance & Assurance, Head of Legal Services and the Executive Assistant of the relevant Strategic Director warning of the failure to respond.
- 3.11 We publish a list of classes of information that are routinely available either free of charge or on payment of a fee. This is called a Publication Scheme.
- 3.12 We will provide access to environmental information through the Environmental Information Regulations 2004 (‘EIR’). Requests under the EIR will be dealt with



in accordance with the [Environmental Information Regulations \(EIR\) Policy](#). In certain cases, an FOI request for information may have to be administered as an EIR request, irrespective of its being identified as an FOI request.

4. Responsibilities and Accountabilities

- 4.1 Managers are responsible for ensuring that this policy is communicated to all employees and that it is adhered to.
- 4.2 All employees must ensure that any request for information they receive is dealt with in line with the requirements of the FOI Act and that they comply with this policy.
- 4.3 Managers are responsible for ensuring all employees complete the mandatory FOI training.

5. Compliance with the Freedom of Information Policy

- 5.1 The Head of Governance and Assurance is responsible for monitoring compliance with this policy.
- 5.2 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](#).

6. Other Relevant Policies, Standards and Procedures

[Information Security Policy](#)
[Data Protection Act Policy](#)
[Data Protection Act guidance on iDerby](#)
[Environmental Information Regulations \(EIR\) Policy](#)
The policy documents are on iDerby or contact the [Information Governance team](#).

The Council is under a legal duty to protect personal data as required by the Data Protection Act 1998 (DPA). The Council will carefully consider its responsibilities under the DPA before disclosing personal data about living individuals, including current and former officers, members, and users of its services.

7. 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