Derby City Council

Personnel Committee
1 December 2016

ITEM 6

Report of the Director of Governance and Monitoring Officer

Data Protection Policy

SUMMARY

1.1 It is the Council's policy to fully comply with the Data Protection Act 1998 and all other related statutory, criminal and civil obligations to which the Council is required to adhere. This applies to the retrieval, storage, processing, retention, destruction and disposal of 'personal information'.

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.

RECOMMENDATIONS

2.1 To note that the Policy will raise awareness to ensure that when collecting and using personal data it is carried out in such a way that recognises the Fair Processing Code, meaning that personal data is obtained fairly, lawfully and with a purpose and legal basis for processing.

2.2 To authorise the adoption and implementation of the Data Protection 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 provide a mandatory e-learning programme as required by the Information Commissioners Office (ICO) to ensure all Elected Members and Staff collecting and using personal data do so appropriately.

2.5 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 and Elected members 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 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 - Organisational Development Manager
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 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 (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 The equality impact assessment is attached to this report and focusses on the positive impact that this policy will have on people with protected characteristics under the Equality Act. The Policy does not mean we cannot do equality monitoring, but it does mean we need to make sure that people are not identified in published equality monitoring reports.

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: Data Protection Policy

Document owner	Richard Boneham, Head of Governance & Assurance
Document author and enquiry point	Angela Gregson
Date of document	September 2016
Version	2.0
Document classification	Official
Document distribution	Published via website
Review date of document	September 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.

Date Issued	Version	Status	Reason for change
	2.0	Draft	Updated

Document Approval

Job Role	Approvers Name	Date Approved
Director of Digital Services	Nick O'Reilly	20 September 2016
Information Governance Group	Head of Governance and Assurance – Richard Boneham	27 September 2016
Conditions of Service Working Party	Director of Governance and Monitoring Officer – 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

Derby City Council

Contents

1. Introduction 7
2. Legislation, guidance and standards 8
3. Data Protection Act 1998 and Derby City Council 8
4. Authorised Users 11
5. Elected Members 11
6. Data Access 12
7. Direct Marketing 12
8. Responsibilities and Accountabilities 12
9. Compliance with the Data Protection Policy 13
10. Other Relevant Policies, Standards and Procedures 13
11. Contact Details 13
Appendix 1 14

1. Introduction

1.1 The Data Protection Act 1998 (DPA) is based around eight principles of good information handling. It applies to all recorded information held by the Council or by someone else on behalf of the Council. The Act gives people specific rights in relation to their personal information and places certain obligations on the Council who are responsible for processing it.

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 It is the Council's policy to fully comply with the Data Protection Act 1998 and all other related statutory, criminal and civil obligations to which the Council is required to adhere. This applies to the retrieval, storage, processing, retention, destruction and disposal of 'personal information'.

1.5 The Council is registered as a data controller with the Information Commissioner's Office (ICO). The registration number is Z548584X.

1.6 Terms of reference within this policy (e.g. 'personal information', 'subject access request') are used with the same intent as the definitions applied within the Data Protection Act 1998.

1.7 The Data Protection Act 1998 applies to personal information processed by any forms of media, including CCTV images, photographs, and digital images. Any processing of such data must be in accordance with the principles of the Data Protection Act and this policy.

2. Legislation, guidance and standards

The Council has an obligation to make sure that all information systems and processes meet the terms of all relevant legislation and contractual requirements, including the:

- Data Protection Act 1998 – also see Appendix 1
- The Caldicott Principles
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Government Security Classification Scheme

If you are not sure of your responsibilities under any of these laws, contact the Head of Governance & Assurance for further information.

3. Data Protection Act 1998 and Derby City Council

By following and maintaining strict safeguards and controls, the Council will:

1. acknowledge the rights of individuals to whom personal data relates and make sure that they can use these rights in accordance with the Data Protection Act 1998.

- ensure all forms ask for explicit consent for the collection of data with the use of an opt-in requirement.

2. ensure that collecting and using personal data it is carried out in such a way that recognises the Fair Processing Code, meaning that personal data is obtained fairly, lawfully and with a purpose and legal basis for processing.
3. ensure that when it collects personal data it will ensure that where required, it will make individuals aware that their information is being collected, the purpose for collecting their information, and whether it will be shared with any third parties. This will be done through the use of privacy notices. When reviewing documents and forms, it will always consider whether a privacy notice should be included.
4. where possible indicate the data retention period when it collects personal data.
5. only obtain and process personal data as specified in our notification.
6. collect and process personal data on a **need to know** basis making sure that it is accurate, not excessive and is disposed of at a time appropriate to its purpose.
7. not process data for a new purpose until the Information Commissioner's Office has been notified of this and the data subjects have been informed and consent has been sought where required.
8. make sure that records are kept up to date and are corrected promptly if they are found to be inaccurate.
9. ensure data is destroyed after the specified data retention period has been reached as indicated at the time it was collected.
10. make sure that for all personal data it takes the correct security measures – both technically and organisationally - to protect against loss, damage or misuse.
11. make sure that the movement of personal data is done in a lawful way, both inside and outside the Council and that it has suitable safeguards at all times.
12. only share data were there are legitimate purposes to do so, with partners who have equivalent data protection measures, with the consent of data subjects and in accordance with relevant guidance including guidance on sharing sensitive financial, medical and personal data.
13. ensure an Information Sharing Agreement is implemented when personal data is to be shared regularly with a third party,
14. take into consideration any statutory basis of any proposed data sharing -if the sharing is justified and how to ensure the security of the information being shared.

15. ensure that personal data is not shared with a third party organisation without a valid business reason and where required it will notify individuals that the sharing will take place in the form of a privacy notice. If any new purposes for the data sharing are to take place, it will seek consent from the individuals concerned.

16. follow all the good practice advice and guidance issued by the Information Commissioner Office.

To support the safeguards and controls the Council will:

- designate a Senior Information Risk Owner responsible for information risk within the authority.
- have an Information Governance Team responsible for gathering and distributing information and issues relating to information security, the Data Protection Act and other related legislation.
- have a designated departmental Information Asset Owner, responsible for issues relating to information security and the Data Protection Act 1998 within their own department.
- ensure that when an inaccuracy has been identified, the service correct it within 5 working days. The Information Governance team will help identify the reason for the inaccuracy and assist in the prevention of a repeat.
- make sure that all activities that relate to the processing of personal data have the correct safeguards and controls to make sure of information security and compliance with the Data Protection Act 1998.
- make sure that all contracts and service level agreements – SLAs – between the Council and external organisations, including contract staff – where personal data is processed - refers to the Data Protection Act 1998 where necessary and is logged onto our contracts registered and is monitored.
- handle any requests for access to personal data courteously, promptly and appropriately, making sure that either the data subject or their authorised representative has the proper right to access under the Data Protection Act 1998.
- make sure that information provided is clear and explicit.
- work towards adopting, as best practice, the key principles of ISO 27001 & ISO 17799 – the International Standard for Information Security.
- make sure Information Sharing Agreements - ISAs - are in place where necessary and when sharing with partner agencies takes place.
- ensure that staff inform the Information Governance team of all existing and new ISAs so that they can be recorded on a register.
- complete Privacy Impact Assessments when considering projects that have significant impacts on individual's data protection rights.
- ensure staff report all security breaches to the Information Governance team within 24 hours.

- manage reported security breaches appropriately and in line with the security breach management framework issued by the ICO.
- introduce a Protective Marking Scheme to classify and protect personal information.
- follow guidance on the sharing of medical, financial and personal records issued by the appropriate bodies responsible for such.

4. Authorised Users

4.1 Authorised users will only have access to personal information where that access is essential to their duties. Authorised users should discuss with their line manager any instance where access rights require clarification. Access rights are not to be regarded as permanent and are subject to change at any time depending upon the nature of the duties being fulfilled by the authorised user.

4.2 Authorised users with access to personal information must be familiar with the requirements of the Data Protection Act 1998.

4.3 Authorised users should only record information about an individual which is relevant, and should be aware that they may be required to justify what has been written and be prepared for that information to be released as part of a subject access request.

4.4 Any authorised user who is found to have inappropriately divulged personal information will be subject to investigation under the Council's disciplinary procedure, which may result in dismissal and possible legal action. Where the authorised user is a Councillor they will be subject to investigation under the Code of Conduct set for councillors

4.5 All authorised users must follow good practice as indicated by the Data Protection Act 1998 and any such codes of practice issued by the Office of the Information Commissioner or the Council, when processing personal data.

5. Elected Members

5.1 Elected members have no automatic rights to access personal information, except, for example, when acting as a member of a committee or acting on behalf of an individual or under their instruction. The requirement for access must be clearly demonstrated at all times.

5.2 Specific guidance will be produced for elected members who require access to personal information, and for employees who receive requests for access in accordance with the best practice guidance issued by the Information Commissioner Office.

5.3 Elected members are bound by the terms of the Data Protection Act 1998 for the duration of their tenure of office. Elected members must, when their term of

office expires or for some other reason they cease to be an elected member, arrange for the transfer or secure disposal of all personal information held by them or their support staff on their behalf.

5.4 Where information is being transferred, the Head of Democracy, or their representative, in consultation with the Head of Governance & Assurance will make the necessary arrangements for the transfer and future management of the information transferred.

6. Data Access

6.1 Authorised users must be aware of what to do when requests for information are made under the Data Protection Act.

6.2 All data subjects have a right of access to their own personal data; the Information Governance Team will provide advice to data subjects about how to request or access their personal data held by us – this is a Subject Access Request.

6.3 Third party personal data will not be released by us when responding to a Subject Access Request unless consent is obtained, it is required to be released by law or it is deemed reasonable to release

6.4 The Information Governance Team is responsible for ensuring that subject access requests are acknowledged and are handled within the legal time limit of 40 days.

6.5 Requests for access to data by the police, other authorities and professionals must be made in writing and where applicable completion of forms specific to their request e.g. Form 807 for police requests

7. Direct Marketing

7.1 The Council will not participate in direct marketing practices where individuals do not consent to the use of their personal information for this purpose.

7.2 All individuals must be given the opportunity to opt-in to receive material at the point of data collection, or opt-out of receiving material at the point of distribution.

7.3 The appropriate opt-in and opt-out mechanisms must be put in place where third party marketing or advertising materials are distributed to named individuals. In situations where this cannot be feasibly done, the materials must not be distributed.

8. Responsibilities and Accountabilities

8.1 Managers are responsible for ensuring that this policy is communicated to all employees including temporary staff and that it is adhered to. It must be

communicated to all elected members, contractors, agents and partners working for or on behalf of the Council.

8.2 All authorised users must ensure that any request for information they receive is dealt with in line with the requirements of the Data Protection Act 1998 and that they comply with this policy.

8.3 Managers are responsible for ensuring all employees complete the mandatory DPA training.

8.4 All elected members, contractors, agents and partners working for or on behalf of the Council must complete the mandatory DPA training.

9. Compliance with the Data Protection Policy

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

9.2 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.

9.3 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.

10. Other Relevant Policies, Standards and Procedures

These can be found 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.

11. 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

Appendix 1

General Data Protection Regulation (GDPR)

The European Parliament has formally approved the EU's general data protection reform package, which includes General Data Protection Regulation (GDPR). It is expected to come into force in May 2018.

Given the referendum result of Brexit, the ICO has stated that 'the Data Protection Act remains the law of the land' until it is repealed or amended but in the event that the UK is not part of Europe, given the referendum result, the 'upcoming EU reforms to data protection law would not apply to the UK'. The ICO does say that if the UK wants to trade with the Single Market on equal terms it would need to prove 'adequacy' in respect of its data protection legislation. Therefore the UK data protection legislation would 'have to be equivalent to the EU's General Data Protection Regulation framework'. Bearing this in mind the ICO considers it necessary to push forward with proposed reforms of UK data protection legislation (as contained within the GDPR) in one way or another.

The ICO has advised that public bodies start to consider the impact the GDPR will have on their organisations. To help unpick the pertinent changes from the new regulation the ICO has published a concise "12 steps to take now"