Leeds City Council
Data Protection Policy

Document Control

Organisation	Leeds City Council
Title	Data Protection Policy
Author	Mark Turnbull, Legal Services
Filename	DPA policyVR1.doc
Owner	Assistant Chief Executive, Planning, Policy and Improvement
Subject	Information Governance
Protective Marking	Not Protectively Marked
Review date	July 2018

For revision history, please see appendix B

1. Introduction

Information is an asset. Like any other business asset it has a value and must be protected. Systems that enable us to store, process and communicate this information must also be protected in order to safeguard information assets. 'Information systems' is the collective term for our information and the systems we use to store, process and communicate it. The practice of protecting our information systems is known as 'information security' which is one of the key themes of the council's Information Governance Framework.

This policy is part of a set of information governance policies and procedures that supports the delivery of the Information Governance Framework. It should be read in conjunction with these associated policies, in particular the Information Security Policy and Protective Marking and Asset Control Policy, and the Information Sharing Policy.

This policy sets out the council's approach to processing personal data under the Data Protection Act 1998, and to dealing with information which is "private" under Article 8 of the Human Rights Act 1998.

2. Scope

This policy applies to everyone who has access to the council's information, information assets or IT equipment. These people are referred to as "users" in this policy. This may include, but is not limited to employees of the council, elected Members of the council, temporary workers, partners and contractual third parties.

All those who use or have access to council information must understand and adopt this policy, and are responsible for ensuring the security of the council's information systems and the information that they use or handle.

The policy relates to the council's approach to processing "personal data" under the Data Protection Act 1998, and to dealing with information which is "private" under Article 8 of the Human Rights Act 1998.

3. Definitions

Definitions of specialist terms which appear in the text of this policy can be found in the jargon buster section of the Intranet.

4. Aims/ Purpose/ Objectives

To make it clear how the council responds to its duties in respect of processing "personal data" under the Data Protection Act 1998, and in respect of "private" information under Article 8 of the Human Rights Act 1998.

5. Policy Statement

The council needs to process personal data and private information in order to deliver many of its services. The council's objective is to use personal data and private information in the most efficient and effective way possible to deliver better services, and to enhance privacy.

The council will strive to:

1. Adopt the least intrusive approach. Where services can be delivered or improved without affecting personal privacy, they will be, recognising that the protection of privacy is part of the social well-being of citizens, and therefore in itself one of the council's functions.

2. Process all personal data fairly and lawfully throughout its whole lifecycle.

3. Ensure that any processing of personal data (including sensitive personal data) can be justified under one or more of the fair processing conditions set out in the data protection legislation, and ensure that any dealing with private information is compatible with the rights in human rights legislation.

4. Ensure that personal data or private information is obtained fairly and in a transparent manner.

5. Use personal data and private information throughout its whole lifecycle in a way which is consistent with the purposes which were communicated at the point of collection, or for other purposes which are legally permitted.

6. Only share personal data or private information where the council has the individual's consent, or where this is lawfully permitted, or where the council is required to do so by law or to comply with a court order. Where there is sharing of personal data or private information without the consent of the individual but which is lawfully permitted, then the council strives to ensure that there is openness and accountability in the process of striking a fair balance between individual rights and the wider public interest.

7. Collect and process only the minimum relevant amount of personal data or private information which is required to fulfil the purpose.

8. Take reasonable steps to ensure the accuracy of personal data and private information and to update it where necessary. The council will check and, where necessary, correct any inaccurate or misleading data or information once it is brought to the council's attention, or alternatively will record the data subject's view that the data is inaccurate.

9. Ensure that personal data and private information are no longer retained once the purpose for processing has been fulfilled. Such data and information will be securely destroyed.

10. Implement data retention policies where applicable.

11. Take appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss or destruction of, or damage to personal data and private information.

12. Not transfer personal data or private information to any country outside the European Economic Area unless that country ensures an adequate level of privacy protection.

13. Provide general information to the public on their rights under data protection and human rights legislation and how these rights can be exercised.

14. Process data and information in accordance with individuals' rights under the data protection and human rights legislation.

15. Respond to all requests from individuals to access their personal data as soon as possible and within forty days of receipt, and in accordance with the council's guidance and procedures.

16. A summary of the key messages of this policy can be found in appendix A.

6. Legislative Context

Information governance sits within a legislative background and a number of Acts of Parliament and international standards influence this policy. Users of council information systems must be familiar with the relevant legislation relating to Information Governance and Data Protection, and must be aware of their responsibilities under this legislation. Further information about the statutory legislation governing aspects of the council's information governance arrangements can be found by following the link from the 'managing information' toolkit.

It should be noted that in some circumstances, instances of misuse may constitute a criminal offence.

7. Roles and Responsibilities

It is important that all users (as defined in the scope of this policy) understand what is required of them and comply with this policy.

Detailed descriptions of information governance roles and responsibilities can be found on the managing information toolkit

Under the council's constitution, Directors are required to designate officers ("practitioners") with specific responsibilities for implementing and ensuring compliance with the data protection and human rights legislation.

The City Solicitor is responsible for preparing policies and strategies for approval, guidance and advice, notifications to and dealings with the Information Commissioner, and monitoring compliance in relation to matters within the scope of this policy.

Therefore, the practitioner for each service is responsible for data protection and human rights compliance generally, and for dealing with subject access requests in accordance with this policy, and also in accordance with guidance and advice provided by Legal Services.

In the event that a member of staff gets a subject access request, then they must send the request to cs.freedom.of.information@leeds.gov.uk, or post it to A76/Freedom of Information, Legal Services, Property & Finance section, Civic Hall, Leeds LS1 1 UR, straight away. The request will then be logged into the corporate requests database, and sent to the practitioner for the relevant service, to deal with.

All members of staff must assist the practitioner for their service by providing them with all relevant information in a timely manner, so as to enable the council to respond to subject access requests as soon as possible, and no later than forty days after receipt of such requests.

A member of staff who holds information which is relevant to a subject access request must not alter, deface, block, erase, destroy or conceal any such information with the intention of preventing its disclosure.

A member of staff must not share personal data or private information with other council services, or disclose such data or information to any other organisation or individual unless they have ensured that it is lawful to do so.

8. Training

This Policy is part of the corporate Information Governance Framework.

Appropriate training will be made available for existing staff that have responsibility for information governance duties.

All staff will be made aware of their obligations for information governance through effective communication programmes.

Each new employee will be made aware of their obligations for information governance during an induction-training programme.

Training requirements will be reviewed on a regular basis to take account of the needs of the individual, and to ensure that staff are adequately trained.

9. Policy Compliance and Audit

Failure to observe the standards set out in this policy may be regarded as serious and any breach may render an employee liable to action under the council's Disciplinary procedure, which may include dismissal. The Disciplinary procedure is part of the Local Conditions of Employment.

Non-compliance with this policy could have a significant effect on the efficient operation of the council and may result in financial loss and an inability to provide necessary services to our customers. Individuals who suffer financial loss by reason of a breach of the data protection rules can claim compensation from the council. In certain circumstances, where there has been a serious contravention of the data protection principles, the Information Commissioner can serve a monetary penalty notice on the council, and this can be up to £500,000. The council will audit its information governance procedures and where practical and proportional, Corporate ICT Services will monitor users' access to information for the purpose of detecting breaches of this policy and/or other council policies and procedures.

Occasionally there may be situations where exceptions to this policy are required, as full adherence may not be practical, could delay business critical initiatives or could increase costs. These will need to be risk assessed on a case by case basis. Where there are justifiable reasons why a particular Policy requirement cannot be implemented, a policy exemption may be requested from the Information Governance Management Board (IGMB) via the Corporate Information Compliance Manager.

It is the duty of all users to report, as soon as practicably possible, any actual or suspected breaches in information security in accordance with the Corporate Information Security Incident Management Policy and procedures

Any user who does not understand the implications of this policy or how it may apply to them, should seek advice from their immediate line manager and/or their directorate's Information Compliance Officer or the Corporate Information Compliance Manager.

10. Policy Governance

The following table identifies who within Leeds City Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** –the person(s) responsible for developing and implementing the policy.

- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Chief Officer, Intelligence and Improvement
Accountable	Senior Information Risk Owner (SIRO) - Assistant Chief Executive, Customer Access and Performance
Consulted	Information Governance Management Board (IGMB), Information Assurance Sub-group, IKM/ ICT Liaison Group, ICT SLT, FOI/DPA practitioners Sub-group.
Informed	All users and persons with management or oversight responsibility for users.

11. Equality Impact Assessment

Equality and diversity issues have been considered in respect of this policy and it has been assessed that a full Equality Impact Assessment is not required as there will be no adverse impact on any particular group.

12. Policy Review and Maintenance

This policy will be reviewed annually, or as appropriate and in response to changes to legislation or council policies, technology, increased risks and new vulnerabilities or in response to security incidents.

13. Declaration

As part of the consultation process this policy has been endorsed by the council's Information Assurance Group, Information Governance Management Board, IKM/ ICT Liaison Group and ICT SLT, and FOI/DPA practitioners Sub-group. In accordance with the council's Information Governance Framework this policy is formally adopted as a council policy.

James Rogers
Assistant Chief Executive (Customer Access and Performance)

Appendix A: Policy Overview and Key Messages

1. This policy sets out the council's approach to processing personal data under the Data Protection Act 1998, and to dealing with information which attracts the protection of Article 8 of the Human Rights Act 1998.
2. This policy reflects the council's legal obligations, and also the council's ambition to adopt the least intrusive approach in its uses of personal data and private information, thereby protecting the privacy of citizens.
3. All members of staff have a part to play. Staff should collect the minimum amount of data and information consistent with the council's purpose, and must assist the practitioner for their service by providing them on request with relevant information, in a timely manner.
4. A member of staff must not share personal data or private information with other council services, or disclose such data or information to any other organisation or individual unless they have ensured that it is lawful to do so.
5. The practitioner for each service is responsible for data protection and human rights compliance generally, and for dealing with subject access requests by individuals.
6. If the council fails to comply with these rules individuals might be able to claim compensation, and the Information Commissioner can fine the council up to £500,000.

Appendix B: Revision History

Version	Status	Revision Date	Summary of Changes	Author
VR	Approved		Signed off by James Rogers	Mark Turnbull
VR1	Final		Amendments made pre-publication on new intranet site	SA / KM

Review and Approvals

Title	Name	Signature	Date of Issue
Information Governance Management Board			
Information Assurance Sub-group			
CTW Policy Steering Group			
IKM/ ICT Liaison Group			
ICT SLT			
Trade Unions			
Members			
Asst CX (Planning, Policy and Improvement)			