Data Protection Policy

Policy Number:	*8.7*	*Version number:*	*01*
Date of issue:	*29th May 2017*	*Date Archived:*	
Reason for policy: *(Redraft/new)*	*Replaces archived Data Protection – Practice & Guidance for Staff (policy No. 5.18)* *New policy to ensure compliance with current legislation*		
Authorised by: _____ ***On Behalf of Management***		*(Signature)*	
Agreed by: _____ ***On Behalf of UNISON***		*(Signature)*	
Agreed by: _____ ***On Behalf of Unite***		*(Signature)*	

N.B. The original copy of this policy containing signatures is held in the Human Resources office.

CONTENTS

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'.

This policy is part of a set of information governance policies and procedures that support the delivery of the CA's functions and it should be read in conjunction with these associated policies. This policy sets out the CA'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. Policy Purpose

To make it clear how the CA 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.

3. Related Policies & Employment Legislation

The main policies linked to this are:

Freedom of Information and Environmental Information Regulations Policy
Information Governance Policy
Information Sharing Policy
Records Management, Retention & Disposal Policy
Subject Access Request Policy

We remain up to date and compliant with all current employment legislation.

4. Scope

4.1. This policy applies to everyone who has access to the CA's information, information assets or IT equipment. These people are referred to as "users" in this policy. The CA is the accountable body for Leeds City Region Enterprise Partnership (LEP) which is also covered by this policy.

4.2. This may include, but is not limited to employees of the CA, temporary workers, secondees, partners and contractual third parties. It is the responsibility of the relevant Head of Service to ensure all data protection training has been completed. All those who use or have access to the CA's information must understand and adopt this policy, and are responsible for ensuring the security of the CA's information systems and the information that they use or handle. The policy relates to the CA'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.

5. Policy Statement

5.1. The CA needs to process personal data and private information in order to deliver many of its services. The CA'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 CA will strive to:

5.1.1 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.

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

5.1.3 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.

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

5.1.5 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.

5.1.6 Only share personal data or private information where the CA has the individual's consent, or where this is lawfully permitted, or where the CA 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 CA 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.

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

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

5.1.9 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.

5.1.10 Implement data retention policies where applicable.

5.1.11 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.

5.1.12 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.

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

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

5.1.15 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 CA's guidance and procedures.

6 Legislative Context

6.1 Information governance sits within a legislative background and a number of Acts of Parliament and international standards influence this policy. Users of the CA's 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. It should be noted that in some circumstances, instances of misuse may constitute a criminal offence.

7 Roles and Responsibilities

7.1 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. In the event that a member of staff gets a subject access request, then they must send the request to freedom.info@westyorks-ca.gov.uk, or post it to Legal and Democratic Services, Wellington House, 40-50 Wellington Street, Leeds, LS1 2DE straight away. The request will then be logged and sent to the relevant service to retrieve the information and respond to the Legal and Democratic Services Team.

7.2 All members of staff must assist by providing Legal and Democratic Services with all relevant information in a timely manner, so as to enable the CA to respond to subject access requests as soon as possible, and no later than forty days after receipt of such requests.

7.3 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. Further details can be found within the CA's Subject Access Request Policy and Procedure.

7.4 A member of staff must not share personal data or private information with other CA 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

8.1 Appropriate training will be given to existing staff that have responsibility for information governance duties.

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

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

8.4 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

9.1 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 CA's Disciplinary, Conduct & Capability procedure, which may include dismissal.

9.2 Non-compliance with this policy could have a significant effect on the efficient operation of the CA 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 CA. 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 CA, and this can be up to £500,000. The CA 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 CA policies and procedures.

9.3 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 Security Incident Management Policy and procedures

9.4 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 the Information Governance Officer.

10 Equality Impact Assessment

In the creation of this policy, consideration has been given to any possible adverse equality impact for the following groups: disability; gender; gender reassignment; marital status (including civil partnerships); sexual orientation; race; religion or beliefs; age; pregnancy and maternity. The policy is considered to have little or no adverse equality impact.

11 Changes to Policy

The CA reserves the right to amend the details of this policy as required following consultation with recognised trade unions and other relevant parties.

This policy will be monitored and reviewed on an annual basis, to ensure that it meets the needs of the CA and ensure compliance with relevant legislation.

A written request can be made to review this policy at any time, by any of the signatories, giving appropriate reasons for requesting the review.