West Yorkshire Combined Authority

Data Protection and Confidentiality Policy

Legal and Governance Services / April 2019
v.1

Introduction

This policy is part of a set of information governance policies that support the delivery of the Combined Authority's functions and it should be read in conjunction with those policies. This policy sets out the Combined Authority's approach to processing person identifiable information ("personal data") to ensure compliance with the data protection legislation.

Related Policies & Legislation

Legislation:

- Data Protection Act 2018 (DPA)
- EU General Data Protection Regulation (EU/2016/679) (GDPR)
- Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (DPPEC Regulations)Freedom of Information Act 2000
- Local Government Transparency Code 2015

Combined Authority policies:

- Freedom of Information/Environmental Information Regulations & Transparency Policy
- Records Management and Data Quality Policy
- ICT Security Policy
- Risk Management Strategy

Combined Authority Procedures

Related Guidance is issued by the Information Commissioners' Office.

Scope

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

This may include, but is not limited to Members of the Combined Authority, and the LEP board, employees, temporary workers, secondees, partners and contractual third parties.

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

Personal Data

The DPA 2018 provides for the regulation of the processing of information relating to individuals and ensures that the standards set out in the EU General Data Protection

Regulation have effect in the UK. The DPPEC Regulations create the "UK GDPR," a single data protection regime that will apply in the UK following its exit from the EU.

Data Protection Policy Statement

The Combined Authority needs to process personal information in order to deliver many of its services. The Combined Authority's objective is to use personal information in the most efficient and effective way possible to deliver better services, whilst ensuring the privacy of individuals is protected.

The Combined Authority will strive to:

1. Adopt the least intrusive approach. Where services can be delivered or improved without affecting personal privacy, they will be.

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

3. Ensure that any processing of personal information (particularly special categories of personal information) is justified on one or other of the legal bases set out in the data protection legislation, and ensure that any processing is compatible with individuals' rights set out in human rights legislation.

4. Ensure that personal information is obtained fairly and transparently by, in particular, the giving of a privacy notice.

5. Use personal information throughout its whole lifecycle in a way which is compatible with the purposes which were communicated at the point of collection or before further processing, or for other purposes which are legally permitted.

6. Only share personal information where the Combined Authority has the individual's consent or where this is legally permitted, or where the Combined Authority is required to do so by law. Where this is done without consent, the Combined Authority ensures 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 information which is required to fulfil the purpose.

8. Take every reasonable step to ensure that personal information is accurate and where necessary kept up to date, and to ensure that inaccurate personal information is erased or rectified without delay.

9. Ensure that personal information is kept in a form which permits identification for no longer than necessary, and that personal information is no longer retained once the purpose for processing has been fulfilled. Such information and information will be securely destroyed, in line with specific data retention policies.

10. Process personal information in a way that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to

personal information using appropriate technical and organisational measures including as appropriate the pseudonymisation and encryption of information, ensuring systems and services are resilient, and availability and access can be restored appropriately, and regularly testing and checking how effective these measures are.

11. Demonstrate responsibility and accountability for all matters in this Policy Statement, keep appropriate records of processing activities and ensure that all personal information is accounted for by an Information Asset Owner (IAO) on the Information Asset Register.

12. Not transfer personal information to any country outside the UK unless that country ensures an adequate level of privacy protection as approved by the UK government, or the Combined Authority has provided appropriate safeguards.

13. Facilitate the exercise of data subject rights, including the right of access, the right to rectify or complete data, the right to erasure (right to be forgotten), right to restriction of processing, right to data portability, right to object, and right not to be subject to a decision based solely on automated processing.

14. Ensure data protection by design, by implementing appropriate technical and organisational measures which are designed to implement the data protection principles above, in an effective manner and to integrate the necessary safeguards into the processing of personal information.

15. Ensure data protection by default, so that by default only information necessary for each specific purpose of the processing are processed, and by default personal information is not made accessible to an indefinite number of people.

16. Use only data processors who provide sufficient guarantees to implement appropriate technical and organisational measures to meet the requirements of data protection legislation and ensure the rights of data subjects are protected.

17. When processing personal data as a data processor, only process the data in accordance with the instructions of the data controller unless otherwise required to do so by law, and not engage another processor without authorisation of the data controller.

18. Notify personal data breaches to the Information Commissioner's Office and communicate personal data breaches to data subjects, as required by data protection legislation.

19. Carry out data protection impact assessments as required by data protection legislation.

20. Ensure the Combined Authority's Data Protection Officer (DPO) is involved in a timely manner is issues relating to the protection of personal information and is accessible to data subjects with regard to all issues about the processing of their information, or the exercise of their rights under data protection legislation.

21. Ensure that users receive appropriate training and guidance on the protection of personal information.

22. Ensure that personal information processed for the purposes of marketing communications is processed in line with the data protection legislation.

23. Co-operate on request with the Information Commissioner's Office.

Confidential Information

It is a principle of law that information received in confidence by a recipient cannot be used to the detriment of the discloser without their consent. A duty of confidentiality can be owed to individuals (in which case the data protection legislation and policy statement set out above will also apply), or it can be owed to legal persons (i.e. commercial legal entities or organisations).

The Combined Authority may be subject to a duty of confidence in the following circumstances:

- Where an express obligation has been imposed by contract (this is more common in commercial situations);
- Where an obligation is implied because of the circumstances of the disclosure (this is determined on the basis of whether a reasonable person standing in the shoes of the recipient of the information would have realised that the information was being given in confidence);
- Where an obligation is implied because of the relationship between the parties (this is more common where individuals are concerned).

There are circumstances in which the public interest overrides an implied or express duty of confidentiality. The Combined Authority is a public authority subject to the requirements of the Freedom of Information Act 2000 which can require the Combined Authority to disclose commercially sensitive and/or confidential information if it is deemed in the public interest to do so.

Confidentiality Policy Statement

The Combined Authority needs to process information including confidential information in order to deliver many of its services. The Combined Authority will

1. Only enter into agreements that bind the Combined Authority to a duty of confidentiality where it is considered to be in the public interest to do so and upon seeking appropriate legal advice.

2. Ensure that express obligations of confidentiality are subject to the requirements of the Freedom of Information Act 2000.

3. Comply with the terms and conditions of agreements for the protection of confidential information.

4. Keep confidential information secret and confidential and secure.

5. Use confidential information only for the purpose it was received.

6. Establish and maintain adequate security measures to safeguard confidential information from unauthorised access or use.

7. Ensure that users receive appropriate training and guidance on the protection of confidential information.

Roles and Responsibilities

All Users

It is important that all users understand what is required of them, comply with this policy, complete any training as directed by their line management and adhere to guidance provided by the Combined Authority. It should be noted that in some circumstances, misuse of personal information or actions by users that prevent data subjects from exercising their rights under the data protection legislation may constitute a criminal offence by individual users.

Users must comply with the following Combined Authority Procedures and Toolkits:

1. Data Protection Impact Assessment Procedure and Toolkit
2. Privacy Notice Toolkit
3. Subject Access Request and Data Subject Rights Procedure
4. Information Sharing Procedure
5. Data Security Incident Procedure

Information Asset Owners

Heads of Service (or Service Managers where no Head of Service is in place) have been designated as Information Asset Owners (IAOs). IAOs are responsible for ensuring that they and all users within their service area comply with this policy and the related procedures and complete all relevant training assigned by the Combined Authority. They operationally own the information contained in their business area and information systems and are responsible for ensuring that their services operate in accordance with this policy. IAOs are required to understand what information is created, received or obtained, how it is held, used and transferred, who has access to it and why. IAOs are responsible for ensuring that all information assets are captured on the Combined Authority's central information asset register, assessing and managing the risks to their information assets, and the appropriate recording and monitoring of risks on their departmental risk register in accordance with the Combined Authority's Risk Management Strategy. IAOs are responsible for investigating data security incidents that concern their information assets.

Information Governance Officer

The Combined Authority's Information Governance Officer (IGO), within Legal and Governance Services is responsible for supporting the Data Protection Officer (DPO),

providing corporate guidance and advice on information governance, including data protection and related legislation and chairing data security incident response meetings in the absence of the DPO. They will assist in the development and maintenance of appropriate systems to support aspects of information governance and to undertake day to day administration relating to enquiries and requests.

Data Protection Officer

The Combined Authority has designated a DPO within Legal and Governance Services. The DPO must be involved in a timely manner in all issues relating to the protection of personal data within the Combined Authority. The DPO can be contacted at Rebecca.BrookesDPO@westyorks-ca.gov.uk

The DPO will inform and advise the Combined Authority of its obligations under the data protection legislation, monitor compliance with the legislation and the Combined Authority's policies, raise awareness of the data protection legislation and this policy within the organisation, ensure that adequate training provision and auditing arrangement are in place and report information risks to the Senior Information Risk Owner. The DPO will advise the organisation on data protection impact assessments, co-ordinate the response to data security incidents and chair incident response meetings, co-operate with the Information Commissioner's Office and act as the Combined Authority's point of contact for all matters relating to personal data.

Senior information Risk Owner

The Director of Corporate Services has been designated the Combined Authority's (SIRO). The role of the SIRO is to coordinate the development and maintenance of information risk management policies, procedures and standards for the Combined Authority, to ensure the Combined Authority has appropriate assessment processes for information risk, to review and agree actions in respect of identified information risks, to ensure that the Combined Authority's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff, provide a focal point for the resolution and/or discussion of information risk issues and to ensure that the Combined Authority and the Governance and Audit Committee is adequately briefed on information risk issues.

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 Combined Authority's Disciplinary, Conduct & Capability Policy, which may include dismissal.

The Combined Authority will audit its information governance procedures and where practical and proportionate, ICT Services will monitor users' access to information, including email accounts for the purpose of detecting and investigating alleged breaches of this policy and/or related 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, the IGO or the DPO.

The Combined Authority's Regulatory and Compliance Board provides strategic direction and plays a key role in decision making on matters concerning the protection of data. The board also monitors resource allocation and provides a point of escalation for risks and data security incidents. The DPO reports monthly to the Regulatory and Compliance Board.

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.

Privacy

Information including personal information will be processed by the Combined Authority in order to meet the Combined Authority's obligations under the data protection legislation. Information held on the Combined Authority ICT systems (including email and all areas of the network drives) and paper records may be accessed by Audit, ICT Services, and Legal and Governance Services to monitor the compliance of users with this policy and address any issues of non-compliance. Information may be shared with the Information Commissioners Office or data subjects where a legal duty to share information arises.

This information will be stored electronically in line with the Combined Authority's retention schedules. For further details, please consult our privacy notice for job applicants and employees which is located on the intranet and the Combined Authority website for job applicants.