North East Local Enterprise Partnership

Data Use Policy 2020-2021

1. Introduction

The North of Tyne Combined Authority (NTCA) is committed in ensuring the data we collect is used appropriately and protected in line with the Data Protection Laws.

This Policy sets out guidance to employees and identifies the underlying basis and legal framework regarding the types of data we process and share.

2. Purpose

The purpose of this policy is to:

i. Describe the principles and policies we have in place for the data we process
ii. Identify the different types of data we use
iii. Describe 'lawful basis' including fair processing and how it applies to our data
iv. Describe the mechanisms as to how we share data

3. Aim

The policy aims to provide confidence that NTCA has the appropriate systems and forms part of a wider system of ensuring a good Information Governance Policy Framework.

4. Scope

The Scope of this policy applies to:

i. Users of the Combined Authority's information systems, including but not limited to employees of the Authority. Employees are defined as those directly employed by NTCA, or on secondment. This also applies to elected members carrying out duties on behalf of the Authority, contractors, consultants, external

auditors and temporary employees;

ii. The Authority's information that is collected in a paper or electronic format;
iii. Information collected by the Combined Authority or member Authorities for use in carrying out the activities of the Combined Authority;
iv. Information transmitted to/shared/collected with Member Councils, Partners and Contractors;
v. The Authority's data and all reports derived from such data;
vi. Programs developed by the Authority's employees or on behalf of the Authority, using the Authority's equipment or personal computers used for home working by Authority's employees;
vii. Combined Authority owned computing devices and any devices such as PDAs (personal digital assistant), which are used to communicate with the Authority's data network;
viii. Paper based and manual records, storage methods and manual data

Note: Assurances have been obtained from North of Tyne Combined Authority (NTCA) member Councils that they have policies and procedures in place that comply with, and compliment, the NTCA Information Governance Policy and associated IT Security and IT Asset Management Policies.

Where information is shared and transmitted to Partners and Contractors working with NTCA or member Councils on behalf of NTCA, assurance/confirmation has to be obtained from them stating that they meet the information governance/data protection requirements covered in this and associated policies (including all new legal obligations and Data Protection Laws).

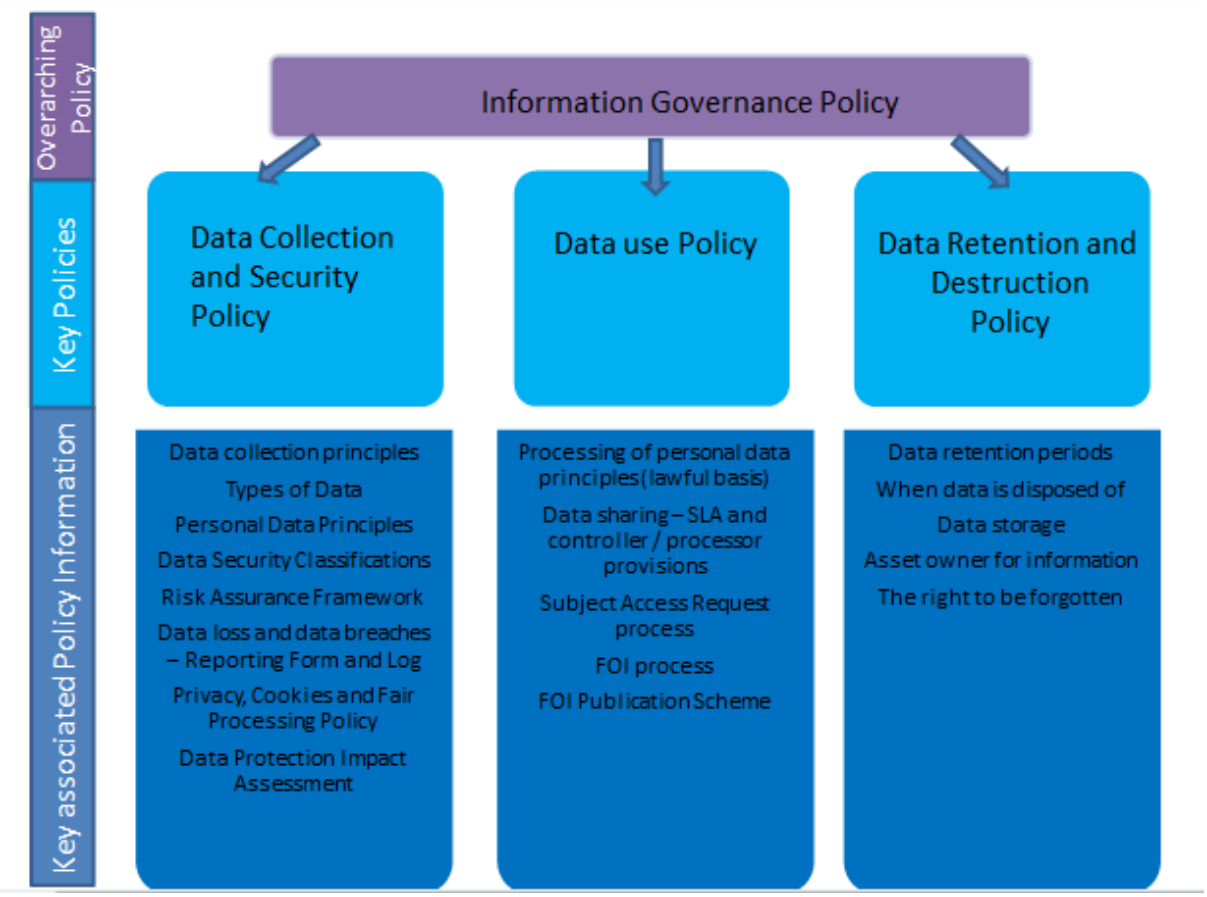
Not all information has the same value or importance and therefore information collected or held by the Combined Authority requires different levels of protection. Information asset classification and data management are critical to ensure that the Authority's information assets have a level of protection corresponding to the sensitivity and value of the information asset. It is therefore vital that all employees and Partners are aware of the importance of our data.

Failure to apply the appropriate controls could result in the alteration, theft, destruction or loss of ability to process data held by the Combined Authority. In addition, some data is of a confidential or sensitive nature. Should this data become compromised then the Combined Authority could face legal action for failing to adequately protect it under the relevant Data Protection Laws.

5. Data Protection and Confidentiality Framework

As described in the Data Protection and Confidentiality Policy (please see separately) the Framework as shown below has been developed to cover all aspects of information governance.

The Data Use Policy focuses on one element of the overarching policy and explores the associated policy information in more detail.



6. Data Processing Activities

NTCA processes various types of data from a wide range of sources including Local Authorities and partner organisations.

The data processed is in accordance with the function and remit of the Combined Authority. In processing data, it is our priority and responsibility that we are able to keep data both safe and secure.

The separate Data Collection and Security Policy introduced the steps employees need to undertake to ensure that security elements are in place for our processing activities, e.g. the Data Protection Impact Assessment (please see the Data Collection and Security Policy for more details). This places an emphasis that data will only be used for the purpose that it was collected.

7. Principles of Processing Data

Data Protection Laws

The Data Protection Laws require the North of Tyne Combined Authority to process data both fairly and lawfully.

The requirement to process data in this manner is set out in the first data protection

principle and is one of eight and such principles that are at the centre of data protection.

All of the principles noted below are designed to protect the interests of the individuals whose personal data is being processed. We ensure that these principles are an underpinning focus of our Information Governance Policy Framework to ensure that we are able to protect the data we collect and process.

Data Protection Principles (as defined by Data Protection Laws):

Principle 1 – fair and lawful

Personal data shall be processed fairly and lawfully.

Principle 2 – purposes

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Principle 3 – adequacy

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Principle 4 – accuracy

Personal data shall be accurate and, where necessary, kept up to date.

Principle 5 – retention

The Act does not set out any specific minimum or maximum periods for retaining personal data. Instead, it says that:

> Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes

Principle 6 – rights

Personal data shall be processed in accordance with the rights of the data subject.

What does Fair Processing mean?

Processing personal data must above all else be fair, as well as satisfying the relevant conditions for processing. “Processing” broadly means collecting, using, disclosing, retaining or disposing of personal data, and if any aspect of processing is unfair, there will be a breach of the first data protection principle – even if you can show that you have met one or more of the conditions for processing.

Fairness generally requires you to be transparent – clear and open with individuals about how their information will be used. Transparency is always important, but especially so in situations where individuals have a choice about whether they wish to enter into a relationship with you. If individuals know at the outset what their information will be used for, they will be able to make an informed decision about whether to enter into a relationship, or perhaps to try to renegotiate the terms of that relationship. Assessing whether information is being processed fairly depends partly on how it is obtained. In particular, if anyone is deceived or misled when the information is obtained, then this is unlikely to be fair.

Information Commissioner’s Office Website (2018)

Lawful Basis for Processing Personal Data

To process personal data we must be able to identify our lawful basis for doing so. The section above described the principles we must adopt and identifying the lawful basis is the next step in the process.

Processing shall be lawful only if and to the extent that at least one of the following applies (in accordance with Data Protection Laws):

(a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;

NTCA Examples:

Example 1: consent being given to use someone’s data (e.g. you may have taken a photograph of someone at an event and you would like to gain consent to use that photograph in a newsletter).

Example 2: A delegate at an event has asked to receive a newsletter. You have a different event coming up that you would like to invite them to them or you have new information to share. **Written Consent** would be needed before you would be able to send the data subject information. In accordance with data protection principles personal data shall only be used in accordance with its original purpose.

(b) processing is **necessary for the performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

NTCA Examples:

Example 1: When commencing employment, a contract will be setup with an individual that will require certain steps that are necessary e.g. the setup of payroll details and the processing of bank details.

(c) processing is necessary for compliance with a **legal obligation** to which the controller is subject;

NTCA Examples:
Example 1: Legislation requires us to meet a legal obligation where the task would be necessary to comply with.

(d) processing is necessary in order to **protect the vital interests** of the data subject or of another natural person;

NTCA Examples:

What are vital interests? These are intended to cover only interests that are essential for someone's life. This generally only applies to matters of life and death.

Example 1: If someone was admitted to hospital on an emergency basis and was unable to give consent to the processing of information then this could be given on a 'vital interests' basis.

(e) processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller;

NTCA Examples:

Example 1: A Councillor carries out a role or function in the public interest in accordance with the requirements of their role.

Consent

Consent is one lawful basis for processing data that NTCA use (as defined in the Lawful Basis section).

It is important that we are able to build trust and engagement and have principles in place that support our aims as the Combined Authority.

In accordance with Data Protection laws, it is important that any activity we undertake that requires consent must be unambiguous and involve a clear affirmative action (an opt-in). For example, signing up to distribution list or newsletter.

Employees must ensure that records are kept that specify consent. Data Protection laws also includes principles to withdraw consent, for example, someone that may sign up to a distribution list for NTCA should be able easily withdraw at any time. In accordance with our Data Retention and Destruction Policy this also identifies that records should be kept in accordance with those that have asked us to remove them

from a mailing list for a period of time (please see the Data Retention and Destruction Policy for further guidance).

8. Data Sharing Protocol and Principles

This section will define the data sharing obligations of the NTCA in accordance with Data Protection Laws. These principles highlight our responsibility of ensuring good governance arrangements and highlights the requirements of laws that written contracts between controllers and processes are a general requirement rather than just a way of demonstrating compliance.

In accordance with Data Protection Laws, as a Data Controller we ensure that:

i. Data is processed effectively and appropriate security measures are in place; and
ii. That processors act on our written instructions
iii. Ensure that people processing the data are subject to a duty of confidence

In accordance with Data Protection Laws, Data Processors are required to:

i. Assist the controller in providing subject access and allow data subjects to exercise their rights under Data Protection Laws
ii. Assist the controller in meeting its obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments
iii. Delete or return all personal data to the controller as requested at the end of the contract
iv. Submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it asked to do something infringing data protection laws of the EU or a member state.

Data Controller Provisions

Where an Authority or NTCA is a separate controller of any Personal Data Processed, each shall comply with its obligations under European Data Protection Law.

An Authority or NTCA shall ensure that any notification to the ICO that may be required under European DP Law is complete and up to date and that it has obtained all necessary consents from Data Subjects to fulfil all of its obligations under any external Contract, including the ability to disclose Personal Data.

Data Processor Provisions

Where an Authority carries out processing on behalf of NTCA, the Authority shall:

a. Process the Personal Data only in accordance with documented instructions from NTCA (including with regard to transfers of Personal Data to a Restricted Country), unless required to do so by European Law to which the Authority is

subject; in such a case, the Authority shall inform NTCA of that legal requirement before Processing, unless that European Law prohibits such information on important grounds of public interest;

b. ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c. taking into account the nature of the Processing, assist NTCA by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of NTCA's obligation to respond to requests for exercising the Data Subject's rights;

d. at the choice of NTCA, delete or return all the Personal Data to NTCA after the end of the provision of services relating to Processing, and delete existing copies unless European Law requires storage of the Personal Data;

e. make available to NTCA all information necessary to demonstrate compliance with the obligations laid down in Data Protection Laws and allow for and contribute to audits, including inspections, conducted by NTCA or another auditor mandated by NTCA;

f. procure that any person acting under the authority of the Authority who has access to Personal Data shall not Process the Personal Data except on instructions from NTCA, unless required to do so by European Law; and

Joint Controller Provisions

If and to the extent that parties are Joint Controllers of Personal Data Processed, Data Protection Laws explain that they shall act in a transparent manner to

determine their respective responsibilities for compliance with the obligations under European DP Law.

Service Level Agreement (SLA) Provisions

Contract Provisions

Where an Authority carries out processing on behalf of NTCA under a Contract, the details of the processing requirements and responsibilities shall be set out clearly.

The details may be updated by written agreement of the parties at any time during the Term.

9. Retrieval and Access Publication

This section details additional responsibilities that the Combined Authority has and the processes involved.

Further details regarding access and retrieval (FOI and SAR as detailed below) can be found in our Privacy, Cookies and Fair Processing Policy on the NTCA Website:

https://www.northoftyne-ca.gov.uk/privacy-policy

The Right of Access

In accordance with the Right of Access principle this gives individuals the opportunity to access information relating to them.

Individuals will have the right to obtain from the Combined Authority:

- Confirmation that their data is being processed
- Access to their personal data

Further detailed guidance will be made available on the NTCA website regarding requesting information from us.

From the 25 May 2018, we must provide a copy of the information free of charge.

Subject Access Request – process

A Subject Access Request (SAR) is any request made by an individual where information is held by the Combined Authority.

In relation to North East LEP matters, a SAR can be made via any of, but not exclusively, to the following methods:

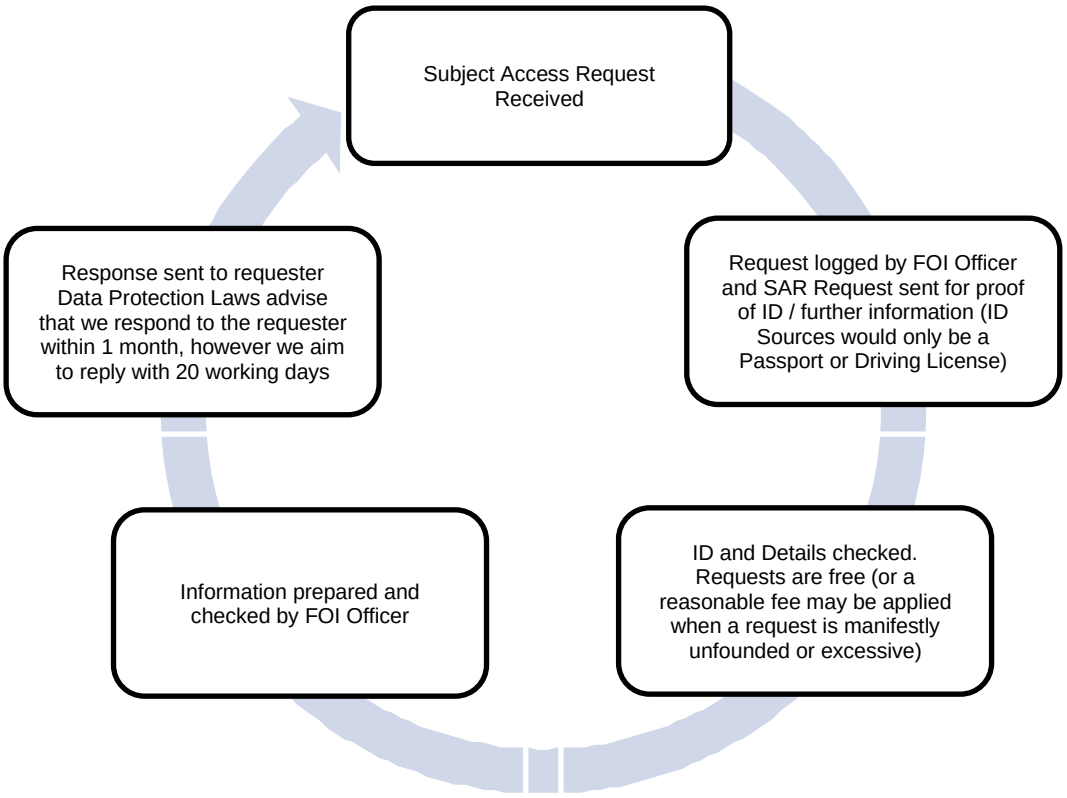
- Email to: DataProtection@northoftyne-ca.gov.uk
- Post:
  NTCA Data Protection Officer
  Floor 6, Civic Centre
  Newcastle upon Tyne
  NE1 8QH

SAR's made online must be treated like any other SAR when they are received, however, the Combined Authority will not provide personal information via social media channels.

The SAR's provide a right for a subject to view their own personal details (as highlighted in the right to access section).

The Combined Authority is not required to respond to requests for information unless it has been provided with adequate and reasonable details.

The diagram below reflects our process for Subject Access Requests.



Freedom of Information Requests – process

The North East LEP's process regarding Freedom of Information Requests is noted below:

Request

- FOI request made to: foi@northoftyne-ca.gov.uk

Process

- FOI team is responsible for North East LEP requests to the Inbox and will contact the appropriate Officer prior to responding

Response

- We are required to respond to the request within 20 working days

NTCA FOI Publication Scheme

NTCA's FOI Publication Scheme commits the North of Tyne Combined Authority and the North East Local Enterprise Partnership 'the North East LEP' to make information available to the public as part of its normal business activities.

The information covered is included our Publication Scheme that is a separate document and will be available on the NTCA website (not at present)**.** The Scheme reflects the classes of information held.

10. Further Information

For further information please contact:

For North East LEP and NTCA matters

John Softly
Monitoring Officer, SIRO

john.softly@northoftyne-ca.gov.uk

For North East LEP matters

Data Protection Officer

DataProtection@northoftyne-ca.gov.uk

Freedom of Information:
foi@northoftyne-ca.gov.uk

For NTCA matters

Philip Slater
Data Protection Officer
Philip.slater@newcastle.gov.uk

Peter Elliott - FOI Officer
foi@northoftyne-ca.gov.uk