# Personal Privacy Policy

City region
Rural powerhouse

# Table of Contents

# 1. Introduction

This policy forms part of York and North Yorkshire Combined Authority's (YNYCA) wider Information Governance Policy Framework, that support delivery of the Combined Authority functions, in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA).

The legislation states that data controllers are responsible for compliance with the six data protection Principles (the Principles) and must be able to demonstrate compliance to data subjects and regulatory bodies. The Information Governance Framework is the York and North Yorkshire Combined Authority's (YNYCA) method to demonstrate compliance with these Principles.

The Personal Privacy Policy sets out how YNYCA will inform Data Subjects about how and why YNYCA uses their data, what measures YNYCA has in place to ensure data disclosures are lawful and secure, and how YNYCA addresses risks to the data protection rights and freedoms of individuals. The Policy is concerned with, in particular, the first, second, and sixth data protection Principles:

> Article 5(1)(a) *Personal data should be processed lawfully, fairly, and in a transparent manner in relation to the data subject.*

> Article 5(1)(b) *Personal data should be collected for specified, explicit, and legitimate purposes...*

> Article 5(1)(f) *Personal data should be processed in a manner that ensures appropriate security of the personal data.*

Queries about this policy, or any policy in the Information Governance framework, should be directed to YNYCA's Data Protection Officer.

# 2. Scope

*Who the policy applies to*

This policy applies to everyone who has access to the Combined Authority's information, information assets or IT equipment.

This policy applies to all YNYCA officers, any authorised agents working on behalf of YNYCA, including temporary or agency staff, elected officials, volunteers, secondees, partners and third-party contractors.

For the benefit of doubt this policy will refer to all individuals within scope of the policy as 'Officers.' Officers who are found to knowingly or recklessly infringe this policy may face disciplinary action in accordance with YNYCA's disciplinary policies and procedures.

*What the policy applies to*

The policy applies to information in all forms including, but not limited to:

- Hard copies of documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email, fax, or electronic file transfer;
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- Information stored on portable computing devices including mobile phones, tablets, cameras, and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images.

In addition, the policy also covers information held by a third party on behalf of YNYCA which is considered to be information held by YNYCA and may be required to be disclosed unless one of the exemptions/exceptions applies.

## 3. Key Messages

1. Under UK GDPR, Data Controllers are required to provide a data subject with a plain English, transparent privacy notice which details the nature of the intended processing, before or promptly after personal data is obtained. YNYCA has adopted a three-tier privacy notice system as recommended by the ICO.

2. UK GDPR compliant consent forms must be issued, signed, and retained for as long as necessary when consent is being used as a lawful reason for processing personal data. This is the responsibility of individual service areas.

3. Routine information sharing with partner organisations should be processed in accordance with an Information Sharing Agreement (which must be signed off on by the DPO). Ad-hoc information sharing should involve a written request where

possible and can be advised upon by the DPO if required.

4. Whenever YNYCA employs an external contractor to process its data (a Data Processor) it must ensure that it has a written contract informing the Processor of what they are permitted to do with YNYCA's data. Categories of Data Processors used must be outlined in YNYCA's corporate privacy notice and individual Processors recorded in YNYCA's corporate information asset register (IAR).

5. A Data Protection Impact Assessment (DPIA) will be conducted for all new projects involving high risk data processing. It is the responsibility of the Service Area to complete DPIAs, with clearance needed by the DPO under certain circumstances.

6. YNYCA operates a structured data protection training programme for all staff in order to reduce the risk of data breaches. This includes general and specialised e-learning modules, as well as bespoke training programmes when necessary (arranged in liaison with/by the DPO).

7. When YNYCA uses Automated Decision-Making Technology it must maintain sufficient safeguards to protect the rights and freedoms of data subjects and must complete a Data Protection Impact Assessment to be signed by the DPO. In order to ensure that decisions are being made fairly, and in accordance with the Data Protection Principles, YNYCA must ensure that the data being input is up to date and accurate.

## 4. Privacy Notices

The UK GDPR states that when a Data Controller is collecting personal data from a Data Subject it must provide that Data Subject with specified information about the nature of the intended processing.

Likewise, if the Data Controller is processing personal data, about a Data Subject, that has been obtained from another source then it must make available, to the Data Subject, specified information about the nature of the processing.

In both cases YNYCA must communicate the specified information, to the data subject, prior to collection or as soon as possible thereafter.

Due to YNYCA's large and varied work it has opted to adopt a three-tier privacy notice system in order to fulfil this requirement. The three tiers being: a corporate privacy notice, a series of service specific privacy notices, and the utilisation of concise 'just in time notices.'

This is an approach recommended in the transparency code of practice issued by the Information Commissioner's Office (ICO).

This Notice will be easily accessible, written in plain English, and will include a glossary of Data Protection terminology so that all YNYCA users are able to understand how YNYCA uses their data.

*Corporate Privacy Notice*

YNYCA will maintain and publish a Corporate Privacy Notice on its website.

The Corporate Notice will state:

- what YNYCA is and who YNYCA's Data Protection Officer is,
- the high-level reasons for requiring personal data,
- a high-level overview of who has access to personal data (internally and externally) – for example, the Police or Anti-Fraud agencies.
- an overview of YNYCA's Information Security arrangements,
- YNYCA's high level lawful basis for data processing and YNYCA's high level data retention policy,
- whether YNYCA stores any personal data outside of the UK especially data outside of the EEA,
- what an individual's rights are over their personal data,
- how they can complain about how YNYCA uses their personal data.

The Corporate Notice will be reviewed and updated by YNYCA's Data Protection Officer on an annual basis or otherwise when required by legislative or regulatory updates.

*Service Specific Privacy Notices*

YNYCA will also maintain and publish Service Specific Privacy Notices as required for each instance of processing. Any such notices will be published alongside the Corporate Notice with the intention that individuals read both notices to achieve a complete understanding of how YNYCA processes personal data.

These notices will state:

- who the Data Controller is and who the Data Protection Officer is,
- what personal data the service processes and the purpose of processing,
- who has routine access to the Personal Data,
- retention periods of the Data,
- the lawful basis for processing.

All Service Specific Notices will contain a link to the Corporate Notice and will be set out in a Questions and Answers format as suggested by the ICO Transparency Code.

Each Service area is responsible for ensuring their Privacy Notice is up to date and readily available. The Data Protection Officer will be responsible for providing a Privacy Notice template, approving all notices, and maintaining a log of notices so that these can be reviewed periodically.

*'Just in Time' Notices*

Just in time notices are to be included on all electronic and paper data collection forms issued by YNYCA. These should state the purpose of collection and where service users can go to find out more information about their Privacy. For example:

| |
|---|
| *YNYCA is collecting your personal data for the purpose of XX. For more information about how and why YNYCA uses your data, including your data protection rights, then please see our website:* |

It is the responsibility of each service area to ensure these notices are utilised.

## 5. Consent Handling Practices

A data subject only consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing, e.g., selecting a tick box. Consent requires confirmatory action so silence, pre-ticked boxes or inactivity will not suffice.

If consent is given in a document that deals with other matters, then the consent must be kept separate from those other matters to be easily distinguished as a separate matter.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to process personal data for a different and incompatible purpose that was not disclosed when the data subject first consented.

Unless there is another legal basis of processing, explicit consent is usually required for processing sensitive personal data, for automated decision-making and for cross border data transfers. Usually, we will be using another legal basis (and will not require explicit consent) to process most types of sensitive data.

YNYCA needs to evidence consent captured and keep records of all consents so that they can demonstrate compliance with legislative requirements.

*Consent Forms*

As well as having a robust and extensive set of Privacy Notices YNYCA must also ensure that its Consent Forms are updated and lawful. The UK GDPR states that when a Data Controller is relying on consent as a lawful basis then the Data Controller has an obligation to provide the Data Subject with a clear statement regarding what the Data Subject is

consenting to. Furthermore, YNYCA must be able to demonstrate consent preferences upon request.

When relying on consent YNYCA will ensure that a consent form is issued to the Data Subject. This consent form must:

- state specifically what the Data Subject is being asked to consent to,
- state where the Data Subject can find out more information about the processing of their Personal Data (i.e., link to Privacy Notice),
- state how long the consent preferences are valid for (including whether consent is valid until preferences are changed by data subject),
- state that the Data Subject can change their consent preferences at any time and provide instructions as to how they can do this,
- include a 'Yes' or 'No' consent tick box,
- include a signature and date box.

Each Service area is responsible for ensuring consent forms are utilised each time YNYCA relies on consent as a lawful basis for Data Processing. Each Service area is also responsible for keeping track of consent preferences and keeping the evidence required to demonstrate consent preferences.

Where possible consent should be given in writing. It is accepted that in some specific situations this will not be possible and YNYCA will have to rely on oral consent. In these circumstances the officer should ensure that this is documented and confirmation sent to the applicant in order to verify their consent preferences.

# 6. Information Sharing

In order to optimise the services that it provides YNYCA appreciates the benefits that information sharing with Partner organisations brings. YNYCA also appreciates that information sharing is not without risk. Therefore, YNYCA will implement measures and safeguards to ensure Information Sharing is conducted lawfully, transparently, and securely.

The process of Information Sharing can be separated into two types of disclosures: routine data disclosures and ad-hoc data disclosures.

*Routine Data Disclosures*

Where YNYCA routinely discloses personal data to other data controllers, an Information Sharing Agreement must be established.

These agreements must detail the lawful basis for processing, how the controllers will comply with the data protection principles, and how the controllers will uphold data protection rights.

Service Areas are responsible for identifying when an agreement is required and are responsible for organising and writing such an agreement.

The relevant Information Asset Owner must sign all Information Sharing Agreements in their service area. If the agreement is considered to be high risk, then YNYCA's Data Protection Officer should also sign the agreement. Where high risks cannot be mitigated *or* where the risks could be considered contentious then the Senior Information Risk Owner (SIRO) may be required to sign the agreement too.

Information sharing arrangements between most North Yorkshire public-sector organisations must use the Information Sharing template(s) stipulated by the Multi-Agency Information Sharing Protocol (see below). The Data Protection Officer will provide a template agreement for arrangements with organisations who are not a signatory to the Protocol.

*Ad-Hoc Data Disclosures*

As well as routine information disclosures, YNYCA will often be required to disclose information to another data controller on an ad-hoc basis. This could be, but not necessarily limited to, to fulfil a legal requirement, for crime prevention and/or detection, or for regulatory purposes.

Where possible, all requests for personal data should be submitted in writing by the requesting data controller. This should state:

- the name and address of the data controller,
- their purpose and lawful basis for processing the personal data,
- whether YNYCA is able to tell the data subject of disclosure,
- how not disclosing the information would prejudice their purpose,
- a counter signature of a senior officer.

When received it is the responsibility of the Service Area to decide if disclosure is appropriate and subsequently arrange for the data to be disclosed. The Service Area may decide to apply limitations to the disclosure.

The Data Protection Officer does not need to be informed of all Ad-Hoc data disclosures but can offer the service area advice and assistance in deciding whether disclosure is appropriate.

Where it is not possible for a request to be made in writing, due to the disclosure being made as part of an emergency situation, then the disclosing officer will gather authorisation from their manager and must obtain a retrospective application which details the above criteria.

Records of Ad-Hoc data disclosure should be kept on the file of the Data Subject so that, if the data subject submits a Subject Access Request, YNYCA is able to easily identify which other organisations have had access to their personal data.

*Multi-Agency Information Sharing Protocol*

YNYCA will become a signatory to the North Yorkshire Overarching Multi-Agency Information Sharing Protocol (MAISP). This Protocol sets out the standards and procedures for information sharing between signatory organisations.

Officers who are routinely involved in data disclosures, or are organising a routine information sharing agreement, should ensure they follow the procedures and best practice laid out in the Protocol & associated pro-formas.

The Data Protection Officer is responsible for representing YNYCA at the Protocol's operational meetings.

## 7. Third Party Data Processors

YNYCA will often employ contractors to carry out data processing activities. These contractors are known as 'Data Processors.' Examples of Data Processors include:

- a software provider who hosts a database for YNYCA,
- Business support service such as Human Resources, Payroll
- Consultants working for YNYCA.

YNYCA employees, or in-house support services are not data processors.

*Contracts*

Whenever YNYCA employs a Data Processor it must ensure that it has a written contract with the processor and that that contract includes a set of Data Processing clauses informing the processor of what they are and are not permitted to do with YNYCA's data.

YNYCA will maintain a set of standard Data Processing clauses for use in contracts. These clauses will include:

<u>Mandatory Details</u>

- the subject matter and duration of the processing,
- the nature and purpose of the processing,
- the type of personal data and categories of data subject,

<u>Mandatory Terms</u>

- the processor must only act on the written instructions of the controller (unless required by law to act without such instructions),
- the processor must ensure that people processing the data (employees) are subject to a duty of confidence,
- the processor must take appropriate measures to ensure the security of processing,
- the processor must only engage a sub-processor (i.e., a third-party organisation) with the prior consent of the data controller and a written contract,

- the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the UK GDPR,
- the processor must assist the data controller in meeting its UK GDPR obligations in relation to the security of processing, the notification of personal data breaches, and data protection impact assessments,
- the processor must delete or return all personal data to the controller as requested at the end of the contract (with an explanation as to method of destruction or return),
- the processor must submit to audits and inspections, provide the controller with whatever information it needs, and tell the controller immediately if it is asked to do something infringing the UK GDPR or other applicable data protection law.

Best Practice

- that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the UK GDPR,
- reference to any indemnity that has been agreed.

YNYCA's procurement procedures will include a process for ensuring that Data Processing Clauses are agreed before the commencement of any data processing activity.

High risk projects may require the sign off of the Data Protection Officer and/or the SIRO prior to the commencement of any data processing activity.

Where YNYCA is being asked to sign Data Processing Clauses, either by a Data Processor or a Data Controller that YNYCA is processing data for, then it is the responsibility of the service area to ensure the contract includes all mandatory and best practice terms. The Data Protection Officer will provide guidance as to what should and should not be in a data processing contract.

*Records of Data Processors*

YNYCA is not obliged to routinely inform data subjects of which Data Processors it employs. However, YNYCA must inform data subjects about the categories of data recipients and as such a paragraph about the use of Data Processors will be included on YNYCA's corporate privacy notice.

YNYCA will keep a record of which data processors have access to personal data within YNYCA. This will be done through YNYCA's corporate information asset register (IAR). The IAR is governed by YNYCA's 'Information Management Policy.'

## 8. Data Protection by Design and Default

YNYCA should embed data protection as part of the design and implementation of services, products, and business practice from the outset.

A Data Protection Impact Assessment ("DPIA") should be completed prior to implementing any system or business change programs that process personal data and is likely to result in a high risk to the rights and freedoms of individuals. Such instances may include:

- use of new technologies (programs, systems, or processes), or changing technologies (programs, systems, or processes);
- use of automated processing, including profiling and data matching;
- large scale processing of special categories of data, or personal data relating to criminal convictions or offences;
- large scale, systematic monitoring of public areas such as CCTV;
- before entering into a data sharing arrangement.

A DPIA must be completed by the Information Asset Owner, seeking advice from the DPO, and should include:

- a description of the processing, its purposes, and legitimate interests if appropriate;
- an assessment of the necessity and proportionality of the processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

In the event of any high-risk data processing, where it is not possible to mitigate the risks to an acceptable level, authorisation from the Information Commissioner's Office may be required. The DPO will advise where this is the case and will liaise with the ICO, following consultation with the SIRO.

The DPO will keep a register of completed DPIAs and ensure that officers have access to a current assessment template.

## 9. Training

Providing officers with comprehensive data protection training has long been recognised as one of the most effective mitigating measures against breaches of confidentiality, integrity, and availability. YNYCA operates and maintains a structured data protection training programme.

*Mandatory Online learning Modules*

All officers who handle personal data as part of their official duties must complete the following mandatory online learning courses provided through E-learning Zone:

- Data Protection
- Introduction to Information Management
- Information Security

The mandatory online learning modules must be completed within the first three months of the officer's employment at YNYCA. It is the responsibility of each employee's manager to ensure that these online learning modules are completed.

YNYCA's Data Protection Officer will liaise with the Organisational Development lead for YNYCA where any changes to/development/procurement of the E-learning mandatory training. YNYCA's Data Protection Officer must approve the training package prior to its use. Any updates or changes to provision of the training must be approved by YNYCA's Data Protection Officer prior to its use.

*Training for Specific Processing Activities (E-learning)*

YNYCA also recognises that some officers will require further training on data protection, and other information governance topics, as their role requires technical knowledge of legislative requirements. The following E-learning packages are available via E-learning Zone to certain officers within YNYCA:

- Freedom of Information
- Information Asset Owners

YNYCA's Data Protection Officer will liaise with the Organisational Development lead for YNYCA where any changes to/development/procurement of the E-learning training. YNYCA's Data Protection Officer must approve the training package prior to its use.

*Training for Specific Processing Activities (Bespoke)*

Where it has been identified that there is a specific requirement for training, but an E-learning module is not available, YNYCA's Data Protection Officer will liaise with the Organisational Development lead for YNYCA to arrange for a training programme to be delivered to the necessary officers.

Examples of such training include, but are not necessarily limited to:

- Handling of Subject Access Requests
- Handling of Data Protection Rights and Complaints
- Secure Redaction of Information
- Data Matching and Profiling
- Law Enforcement Processing
- Surveillance Processing

## 10. Automated Decision-Making Technology Safeguards

When YNYCA utilises Automated Decision-Making Technology it is obliged to ensure that it maintains sufficient safeguards to protect the rights and freedoms of data subjects.

YNYCA's 'Data Protection Rights' Policy details how YNYCA will deal with a Data Subject's rights to be informed of, and object to, Automated Decision-Making Technology.

*Definition and Scope of Automated Decision-Making Technology*

The Information Commissioner's Office defines Automated Decision Making as using automated algorithmic technology to make predictions or decisions about an individual based on data about their personality, behaviour, interests, or habits.

This policy does not apply to automated analysis processing where aggregated data is being used for research, to generate statistics, or to direct YNYCA policy.

The policy also does not apply to processing where automated technology has been used for a calculation but there has been human review before a decision is made i.e., an assessment tool.

*Data Integrity and Algorithmic Integrity*

In order to ensure that decisions are being made fairly, and in accordance with the Data Protection Principles, YNYCA must ensure that the data being input is up to date and accurate. Where possible YNYCA will allow Data Subjects to input their own data. Where this is done the data field descriptions must be clear, concise, and must not be misleading.

Where YNYCA officers are inputting personal data from other existing records they must carry out and record checks to ensure that the data is correct, up to date, and relevant for the purposes of processing. Officers must also ensure there are no legal restrictions to the use of automated decision making. Where possible, any legal restrictions will be noted on the Data Subject's main file.

Likewise, when using algorithmic technology, YNYCA must be able to guarantee the quality of the algorithm and must be able to understand the algorithmic calculation should the Data Subject lodge an appeal. Algorithmic technology must be procured, with proper procurement checks taking place, before being utilised.

*Data Risks*

YNYCA Officers must complete a Data Protection Impact Assessment prior to the use of Automated Decision-Making Technology. The DPIA will assess any data risks associated with the processing.

As Automated Decision Making Technology is generally considered to be 'high risk,' the Data Protection Officer must sign and authorise the DPIA prior to the commencement of the processing.

*Data Processors Using Automated Decision-Making Technology*

Where YNYCA employs a Data Processor to utilise Automated Decision-Making Technology it must ensure it has completed and had approved a Data Protection Impact Assessment,

agreed to Data Processing clauses, and agreed a process of appeals prior to the processing taking place.

YNYCA will record all instances of Data Processors using Automated Decision-Making Technology on its Information Asset Register and Register of Automated Decision-Making Technology.

## 11. Policy Review

This policy will be reviewed every two years unless there is a change in legislation, practice or procedure in which case the policy will be reviewed more frequently to ensure it remains accurate, relevant and up to date.