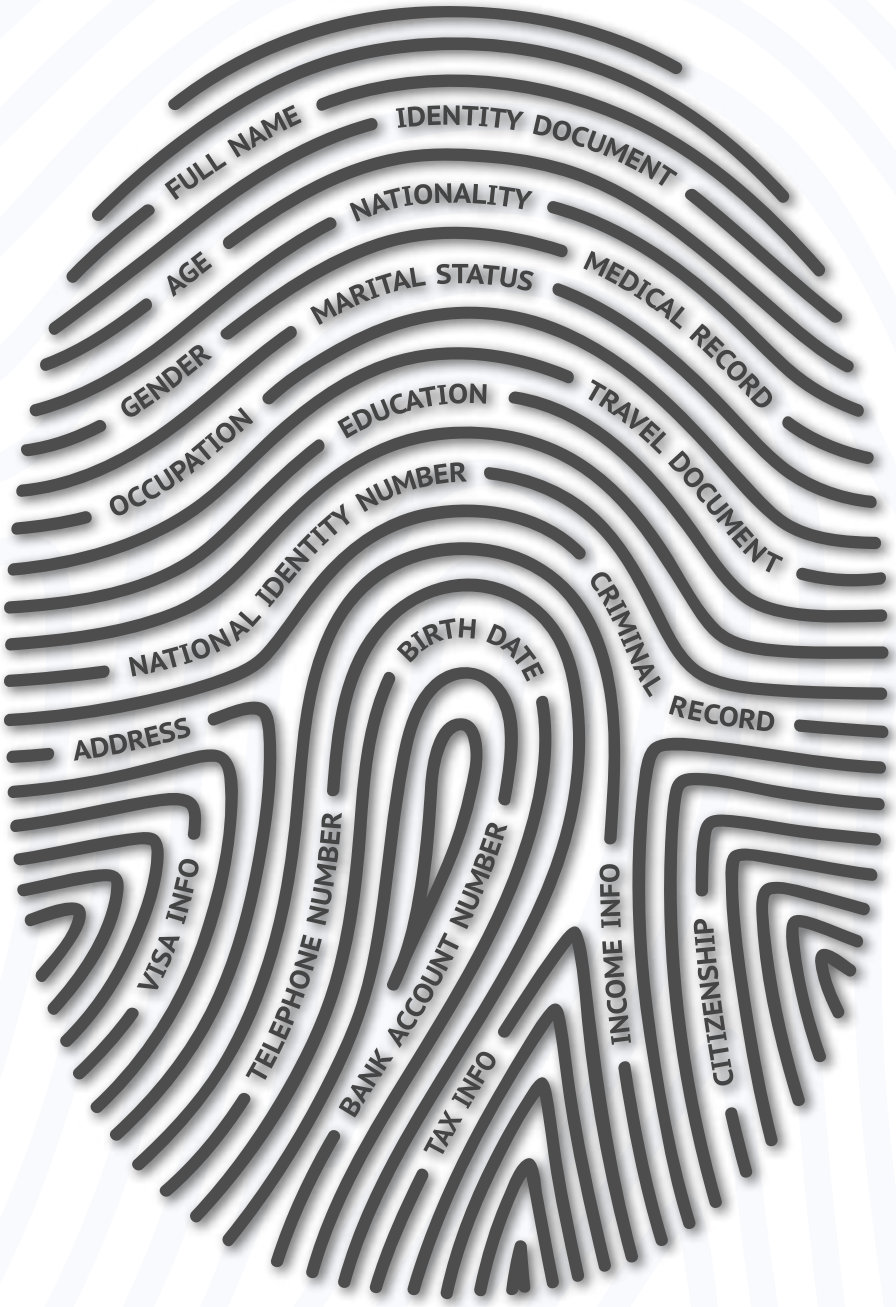
# Stockton-on-Tees Borough Council
# Information Governance

# Data Protection Policy




Stockton-on-Tees
BOROUGH COUNCIL

# Document Control

| | |
|---|---|
| **Document name** | Data Protection Policy |
| **Author** | Business Partner Information Governance |
| **Department** | Information Governance |
| **Document Status** | Approved |
| **Approval** | May 2019 |
| **Publication date** | July 2019 |
| **Review date:** | Annually |

# Version Control

| Version | Date | Amended by | Comments |
|---|---|---|---|
| 1.0 | May 2019 | | Approved CGWG |
| 2.0 | October 2021 | Information Governance Manager | Reviewed October 2021 |
| | | | |
| | | | |

# Distribution

| Version | Date | Comments |
|---|---|---|
| 1.0 | September 2019 | Approved CGWG |
| | | |
| | | |
| | | |

# STOCKTON-ON-TEES - GOVERNANCE FRAMEWORK

This document forms part of the Stockton-on-Tees Borough Council wider Governance Framework which sets out the arrangements that are in place to ensure that the intended outcomes for our stakeholders are defined and achieved and that governing bodies and employees are always working ethically and with integrity to achieve the organisation's objectives, whilst acting in the public interest at all times.

The Council's information governance arrangements recognise the importance of reliable, accurate information to support the provision of good quality services, compliance with current legislation and regulations as well as demonstrating trust in the Council to maintain both confidentiality and security of personal information.

The objective of this framework is to set to how the Council will improve its information governance by establishing:

- Core measures to protect personal data and other information across the Council
- Stronger accountability mechanisms within the Council
- A culture that properly values, protects and uses information
- Stronger scrutiny of performance

# LINKED POLICIES WITHIN INFORMATION GOVERNANCE

| | |
|---|---|
| **Records Management Policy**<br>**Retention and Destruction Policy** | **Data Protection Policy**<br>**Freedom of Information Policy**<br>**RIPA Policy**<br>**Data Subject Access Policy**<br>**Positive Feedback and Complaints Policy** |
| **Information Security Policy**<br>**Good Governance Guide** | |

# Contents



# 1. INTRODUCTION

1.1 This policy sets out Stockton-on-Tees Borough Council's ('the Council') approach to compliance with its duties under the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulations (UK GDPR).

1.2 The Data Protection Act 2018 and the UK General Data Protection Regulations regulates the way in which personal data about individuals is processed, including collection, storage, use, disclosure, length of time retained and destruction controls. This applies whether personal data is held electronically on an IT system, in the cloud, in a paper format, as CCTV footage or a photograph.

1.3 The Council is registered with the Information Commissioner's Office (ICO, "The Regulator") as a data controller for the processing of personal information. Its registration number is Z590889X.

1.4 The Council also holds separate registrations for some other functions undertaken by the Council and its employees, for example: Electoral Registration and the Returning Officer; Superintendent Registrar.

# 2. PURPOSE

2.1 This Data Protection Policy states the Council's intention to ensure compliance with the principles relating to the processing of personal data as set out in Article 5 of the Data Protection Act 2018.

2.2 The policy incorporates guidance from the ICO and outlines the Council's overall approach to its responsibilities under the DPA 2018 and the UK GDPR.

# 3. POLICY STATEMENT

3.1 Personal information / data must be dealt with appropriately and within the law however it is collected, recorded or used. The Council will treat personal information lawfully in accordance with the legislation and ensure this approach is embedded throughout all council departments and those detailed within the scope of this policy.

3.2 The Council, as a registered data controller, processes personal data and sensitive personal data of people it deals with to carry out its statutory duties, perform its functions and to comply with the terms of any contracts it has entered into. This includes information on current, past and prospective service users, employees, suppliers, clients, customers, and others with whom it communicates. It may also include all persons who live, work or visit the Borough.

# 4. SCOPE

4.1 This policy applies to all employees (including elected members, temporary, casual, or agency staff, contractors, consultants and suppliers with whom we have a contractual relationship) working for or on behalf of the Council, third parties and others who may process personal information on behalf of the Council.

4.2 The policy covers staff who may be involved in Electoral Registration or the delivery of elections or referendums; acting on behalf of the Electoral Registration Officer or the Returning Officer, including temporary staff employed as part of the annual canvass of electors or running of an election.

4.3 The policy covers other parts of the organisation who may be registered as separate controllers with the ICO but operate as part of the Council. For example; staff who act on behalf of the Registrar's service, including temporary staff involved in the registration of Births, Deaths, Marriages and Civil Partnerships as well as Citizenship.

# 5. DATA COVERED BY THE POLICY

5.1 This policy covers the processing of personal data relating to a living individual, processed wholly or partially by automated means (electronically) or processing of personal data other than by automated means, (manually) i.e. data which forms part of a manual filing system or intended to form part of a filing system. In summary, personal data held manually and/or electronically, data compiled, stored or otherwise by the Council, or by a third party on its behalf.

5.2 The policy covers both personal data and sensitive personal data, known as special category data, as determined by the DPA 2018 and UK GDPR. It covers the collection, storage, processing and distribution of personal data. It gives rights to the individuals about whom information is recorded. It allows individuals to find out what information is held about them and the purpose for which it is held.

# 6. DEFINITIONS

6.1 Definitions used in the Data Protection Act & UK GDPR and in this policy are as follows:

i '*Personal data*' is any information relating to an identified or identifiable natural person, either through their name or another identifier such as an identification number.

ii '*Processing*' refers to any operation performed on personal data, whether manually or electronically or automated; such as collection, use, storage, disclosure or destruction.

iii '*Data subject*' is the term used to describe any given person when identified in relation to their personal data.

iv The '*data controller*' is the organisation which decides how and why personal data is used, while the 'data processor' is the organisation/ person responsible for processing personal data on behalf of the Controller. Stockton-on-Tees Borough Council is a data controller, while its suppliers are data processors.

v '*Special categories*' of personal data encompass ethnicity and data concerning health, among other categories.

# 7. THE PURPOSE OF THE DATA PROTECTION ACT 2018

**The Principles of the Data Protection Act 2018**

7.1 The Data Protection Act 2018 has set out requirements on how organisations can process personal data. It has six principles which are:

- Personal data shall be processed lawfully, fairly and in a transparent manner;
- Personal data shall be collected for specified, explicit and legitimate purposes;
- Personal data shall be adequate, relevant and limited to what is necessary in relation to those purposes;
- Personal data shall be accurate and, where necessary, kept up to date;
- Personal data shall be kept in a form that identifies the individual for no longer than is necessary;
- Personal data shall be processed in a manner that ensures appropriate security of the personal data.

The Council will meet the requirements of the data protection principles as follows:

**Principle 1: Data is processed lawfully, fairly and in a transparent manner**

a. The Council details on its Information Asset Registers all data that the Council holds, citing the use / purpose of the data, the legal basis for processing it and the conditions under which it is processed. The Council's Privacy Notice sets out how and why the Council processes personal data and provides a transparency to its users that data is processed in accordance with the Data Protection Act 2018 and the UK GDPR. It provides a clarity to the data subject about their rights with respect to the processing of their data.

b. The Information Asset Registers are regularly reviewed and updated.

c. Individuals have the right to access their personal data and any such requests made to the Council shall be dealt with in a timely manner.

**Principle 2: Data is collected for specified, explicit and legitimate purposes.**

a. All data is processed by the Council using one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.

b. The Council shall record the appropriate lawful basis for each data set on the Information Asset Registers.

c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent will be clearly available and systems will be in place to ensure the data is removed.

**Principle 3: Adequate, relevant and limited to what is necessary in relation to those purposes**

a. The Council will only collect personal data that is needed for the specified purposes.

b. The Council will periodically review the data it holds and delete data according to the Records Management Retention Schedule.

**Principle 4: Accurate and, where necessary, kept up to date**

a. Reasonable steps will be taken to ensure the personal data held is not incorrect or misleading. If personal data is incorrect or misleading, steps will be taken to correct or erase it as soon as possible.

b. Personal data will be kept up to date as required.

c. The Council will comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data in accordance with the conditions set out in the UK GDPR.

**Principle 5: Kept in a format that identifies the individual for no longer than is necessary**

a. Personal data will not be kept for longer than necessary and the data shall be deleted in line with the Council's Records Management Retention Schedule.

b. In certain circumstances it may be appropriate to retain the information longer than initially required. For example, a pending or actual legal action, change of legislation or regulation or legitimate business need, research, Government returns or analysis and evaluation. In such instances the data will either be anonymised or pseudonymised so that the individual is no longer identifiable from the data.

c. The Council will regularly review the information it holds and erase or anonymise personal data when it is no longer required for the purpose it was obtained.

d. Individuals' requests for erasure under 'the right to be forgotten' will be considered and deleted if appropriate conditions are met.

e. Any personal data to be kept for public interest archiving, scientific or historical research, or statistical purposes will be clearly identified.

**Principle 6: Processed in a manner that ensures appropriate security of the personal data**

a. Personal data is kept securely, supported by a number of technical and organisational measures including: secure on site and off site electronic storage, encryption, secure electronic system sign on authentication, Malware, secure building access, secure on and off site paper storage, staff training and guidance.

b. Access to personal data shall be limited to individuals who need access and appropriate security will avoid unauthorised sharing of information.

c. When personal data is deleted this will be undertaken safely and ensure that the data is irrecoverable.

d. Appropriate back-up and disaster recovery solutions are in place.

e. Individuals will be notified if their data is accidentally or unlawfully destroyed, lost, altered or disclosed which presents a high risk to individuals rights and freedoms.

# 8. THE COUNCIL'S RESPONSIBILTY

8.1 As a data controller, the Council has an appointed Data Protection Officer to handle day to day issues which arise and to provide employees with advice, guidance and training on data protection issues. The Council will:

- Ensure all employees are aware of their responsibilities under the Data Protection Act.
- Provide regular mandatory data protection awareness training to all Council employees and Elected Members to ensure they understand their responsibilities.
- Ensure that all Council partners understand their responsibilities and are made aware of the Council's Data Protection Policy.

# 9. INDIVIDUALS ROLES AND RESPONSIBILITIES

9.1 The Data Protection Officer (DPO) in conjunction with the Council's Senior Information Risk Owner (SIRO) will have overall responsibility for the implementation of this policy and for reporting any data breaches to the ICO within the relevant timescales.

9.2 All Corporate Management Team (CMT) are responsible for implementing data protection procedures within their Directorates. The Information Asset Owners (individuals who have been identified as having the overall responsibility of the information and ensuring it is being held for a lawful purpose) will take responsibility for ensuring data protection principles are being applied to the data being processed. Information Asset Registers will be used to list all personal information held.

This will be kept up to date and monitored on a regular basis.

9.3 Where an Elected Member has access to and processes personal information on behalf of the Council, the Member does so under the Council's 'registration' and must comply with this policy. When Members process personal data whilst acting as a Ward Councillor, they do so as data controllers in their own right.

9.4 Employees are expected to:

- Familiarise themselves and comply with the data protection principles.
- Familiarise themselves and comply with information governance policies.
- Familiarise themselves with the Councils data breach procedures.
- Undertake mandatory e-learning and refresher training.
- Ensure any possession of personal data is up to date and accurate.
- Keep personal data for no longer than is necessary.
- Ensure personal data is only used for the purpose for which it is requested.
- Ensure personal data is processed securely.
- Dispose of personal information securely.
- Ensure they only access personal information to which they have a legal entitlement in connection with their role in the organisation.
- Ensure there is a lawful condition for collecting, sharing, or disclosing personal data.
- Contact the Data Protection Officer or Information Governance team for any concerns or doubt relating to data protection to avoid infringement of the DPA 2018.
- Report any data breaches as soon as possible to the Information Governance Team.

# 10. DATA SECURITY AND DATA BREACHES

10.1 All staff are responsible for ensuring that personal data which they process is kept securely and not disclosed to any unauthorised person or organisation. The transferring of personal data must be undertaken securely. Access to personal data will only be given to those who can demonstrate a lawful basis for requiring the data. Personal data will not be shared across service departments unless there is a lawful basis to do so.

10.2 Personal data will not be left where it can be accessed by persons not authorised to see it.

10.3 Staff and Elected Members who work away from the office must have particular regard to the need to ensure compliance with this policy. The security of processing of data outside Council premises, usual places of work and whilst travelling, must be ensured.

10.4 The Data Protection Officer will ensure data breaches are investigated and where the breach is likely to pose a risk to the rights and freedoms of individuals, reported to the Information Commissioner's Office, in line with the requirements of the legislation.

10.5 Personal data which is no longer required will be destroyed confidentially using the Council's preferred disposal method. This will be undertaken in a timely manner and in accordance with the Records Management Retention Schedule.

10.6 Data breaches or suspected data breaches should be reported immediately to informationgoverance@stockton.gov.uk email account. An Officer will be allocated to support an investigation into the circumstances around the data loss. An action plan to mitigate against a re-occurrence will be put in place alongside wider sharing of the learning.

# 11. INFORMATION SHARING

11.1 Personal data may need to be shared with third parties to deliver services or perform Council duties. The Council will only share personal data when there is a lawful basis to do so, where it is necessary to achieve a clear purpose and it is fair and proportionate to do so. This will include sharing information appropriately should there be any safeguarding concerns.

11.2 Where appropriate, Data Sharing Agreements (DSA) will be in place to support the sharing of information with third parties, unless a contractual agreement is in place. All Data Sharing Agreements must be signed off by the appropriate Service Manager and sent to the Information Governance team. The Information Governance team will keep a register of all Data Sharing Agreements and ensure these are reviewed on a regular basis.

# 12. DATA PROTECTION BY DESIGN AND DEFAULT

12.1 The Council will embed data protection as part of the design and implementation of services, products and business practice from the outset.

12.2 Data Protection Impact Assessments (DPIAs) are used to embed data protection into the design of services, for example in instances when the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals. Such instances may include, but are not limited to:

- Introduction of new technologies;
- Systematic and extensive processing activities;
- 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; and
- Before entering into a data sharing agreement.

In addition to the above, appropriate technical and organisational measures designed to implement the data protection principles and safeguard individual rights will be put in place.

Some examples of how Stockton-on-Tees Borough Council will do this are listed below:

- minimise the processing of personal data;
- pseudonymise or anonymise personal data as soon as possible;
- ensure transparency in respect of the functions and processing of personal data; and
- create security features.

# 13. THE RIGHTS OF INDIVIDUALS

13.1 The Data Protection Act 2018 gives rights to individuals in respect of personal data held about them. This applies to all individuals including Elected Members, Council employees and members of the public. Each individual has the right to:

- be informed about how and why their personal data is processed;
- access their data;
- the rectification of their data;
- the erasure of their data;
- restrict processing of their data;
- data portability;
- object to the processing of their data; and
- not be subject to fully-automated decision-making including profiling.

For more information about the rights of the individual please visit our website on **www.stockton.gov.uk/our-council/good-governance-doing-things-properly/data-protection-and-access-to-information/**

13.2 The Data Protection Officer will ensure appropriate processes are in place to allow individuals to exercise their rights, according to the provisions of the Act.

**Accessing Personal Data**

13.3 Individuals have the right to access their personal data and any such requests made to the Council shall be dealt with in a timely manner. Information requests and data subject access requests are processed by the Information Governance team. Individuals will be expected to submit requests via **foiandcomplaints@stockton.gov.uk** and provide any necessary proof of identification as part of the request.

13.4 The Council aims to respond promptly to these information requests within the statutory time limit. Requests will be managed and tracked by the Information Governance team.

# 14. HOW TO COMPLAIN

14.1 Individuals have the right to contact the Council if they believe their data has been misused or has not been kept secure. This can be done via **www.stockton.gov.uk/complaints** or write to:

**Information Governance Team**

**Information and Improvement**

**Municipal Buildings**

**Church Road**

**Stockton-on-Tees**

**TS18 1LD**

If individuals remain unhappy with the response they can contact the Information Commissioner's Office (ICO) via **casework@ico.org.uk** or write to:

**Information Commissioner's Office**

**Wycliffe House Water Lane**

**Wilmslow**

**Cheshire**

**SK9 5AF**

# 15. MONITORING AND REVIEW

15.1 This policy will be monitored and updated as required in accordance with any change in legislation and good practice guidance.

Stockton-on-Tees
BOROUGH COUNCIL