**Data Protection Act Policy**

**Status/Version: Approved v 4.3**

**Classification: OFFICIAL**

# Objective

## Coventry City Council is required to process relevant personal data regarding members of staff and range of service users. This policy sets out our commitment to protecting personal data and how we will ensure that staff understand how to handle data they have access to a part of their work.

# Scope

## This policy applies to anyone working with personal data that is controlled or processed by or on behalf of Coventry City Council including and not limited to Council employees and service providers.

## Personal information means any data or information, in paper or digital format, relating to a living individual.

# Data Protection Principles

## Coventry City Council will comply with the Data Protection Act 2018 and UK General Data Protection (UK GDPR) principles and ensure that personal data is:

* Processed fairly and lawfully and in a transparent manner
* Obtained for one or more specified, explicit and lawful purposes
* Adequate, relevant and only limited to what is required
* Accurate and where necessary kept up to date
* Not kept in a form which permits identification of data subjects for longer than is necessary
* Processed in accordance with the rights of data subjects
* Processed in a manner that ensures appropriate security of the personal data.

# General requirements

## Some requirements under the DPA and UK GDPR are:

* Personal data should only be accessed by those who need to for work purposes
* Personal data should not be divulged or discussed except when performing normal work duties
* Personal data must be kept safe and secure at all times, including at the office, public areas, home or in transit
* Personal data should be regularly reviewed and updated
* Queries about data protection, internal and external to the Council must be dealt with effectively and promptly

# Information Sharing

## Personal data may need to be shared with other organisations in order to deliver services or perform our duties. This can only be done where we have permission or there is legal obligation for us to share.

## Personal data can be shared within the Council or with other third parties and the sharing can be:

* “Systematic” or routine information sharing where there is an established purpose or
* “Exceptional” or one-off decisions or example in conditions of real urgency.

## Information Sharing Agreements should be completed when setting up ‘on-going’ or ‘routine' information sharing arrangements with third parties. However, they are not needed when information is shared in one-off circumstances but a record of the decision and the reasons for sharing information should be kept.

## All Information Sharing Agreements should be signed off by the Data Protection Officer and a register of all Information Sharing Agreements maintained.

1. **Data Protection Impact Assessments (DPIAs)**

## DPIAs will be completed in these situations to help identify and minimise risks to individuals and must be completed in the following situations that involve personal data:

* At the beginning of a new project or when implementing a new system
* Before entering a data sharing agreement
* When major changes are introduced into a system or process
1. **Subject Access Requests (SARs)**

## The Council recognises that access to personal data held about an individual is a fundamental right provided in the Act and will ensure that all requests from individuals to access their personal data are dealt with as quickly as possible and within the timescales allowed in the legislation.

## Individuals will be expected to submit SARs in writing and provide any necessary proof of identification as part of the request. Under the UK GDPR the Council is not required to charge for these requests.

1. **Complaints**

## Anyone who feels that the Council has broken the law in any way, can complain. Examples of this are when they think their information has not been obtained fairly, it has not been handled securely or they have asked for a copy of their information and they are not happy with the Council’s response.

## Individuals who consider that data is inaccurate or out of date may also request, in writing, that the information be corrected or erased. They will receive a written response indicating whether or not the Council agrees and if so, the action to be taken.

## Individuals can also ask the Council to stop handling their personal information if they think this will cause them harm or distress. This is not always possible. Data Protection Act complaints are initially dealt with by the Information Governance Team.

# Training

## Data Protection training is important so that all staff and agency workers understand their responsibilities. All employees (including temporary employees) must complete the mandatory e-learning training annually.

## Other staff with additional responsibilities should complete relevant training such as the online Subject Access Request Handling training.

# Non Compliance

## Serious breaches of this policy caused by deliberate, negligent or reckless behaviour could result in disciplinary action and may even lead to criminal prosecution.

## Where those breaching the policy are not council employees, this will be regarded as a breach of contract and may lead to termination of their contract.

# Policy Review

## The Information Governance Team has direct responsibility for co-ordinating the maintenance and review of this policy annually.

## Reviews will take into account changes in legislation, best practice, lessons learnt and input from specialist ICT areas within the Council and in consultation with relevant IT service providers.

# Further Information and guidance

## This policy is supported by guidance available on the Council’s intranet pages.

## The ICO has more detailed guidance on their website at [www.ico.org.uk](http://www.ico.org.uk)

## Enquiries regarding this policy should be directed to the Information Governance Team at infogov@coventry.gov.uk or phone (024) 7683 3323

# Related Documents

* Data Handling Policy
* Data Sharing Policy
* Data Protection Impact Assessment Guidance
* Records Management Policy
* Data Breach Reporting Process

**Document Control:**

**Version History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Status | Date | Author | Summary of Changes |
| 1.0 | Approved | April 2000 | M Gordon |  |
| 2.0 | Approved | 24 August 2009 | J Hutchings |  |
| 3.0 | Approved | March 2015 | J Hutchings | Removed excessive sections, e.g. ‘Other Relevant Documents’, ‘Risks’, ‘Definitions. |
| 3.01 | Approved | June 2016 | R. Kotonya | Added information sharing, PIA, complaints and annual review requirements |
| 4.0 | Approved | September 2017 | R. Kotonya | Added more details on training, SARs, requirement and non-compliance, renamed removing statement from title |
| 4.1  | No Approval sought as minor Change due to ICO Recommendation | February 2018 | S. Lock | Added ‘Related Documents’ |
| 4.2 | No Approval Sought as minor update to show **‘UK’** GDPR. SL  | February 2021 | S. Harriott | Updated to reflect UK GDPR – **Approved March 2021 – S. Lock** |
| 4.3 | No approval sought as minor update to related documents | June 2022 | A West | Update to related documents |

**Reviewers**

|  |  |  |
| --- | --- | --- |
| Name | Role | Business Area |
| S. Lock  | Head of Information Governance and Records Manager | Information Governance |

**Management Approval**

|  |  |  |
| --- | --- | --- |
| Name | Date | Version No. |
| Information Management Strategy Group | September 2017 | 4.0 |

**Distribution**

|  |  |  |
| --- | --- | --- |
| Name | Organisational Department | Format |
| All | Coventry City Council | PDF Document via Intranet and Internet |