

Warwickshire County Council

# **DATA PROTECTION and PRIVACY POLICY**

**Approved v1**



# Data Protection and Privacy Policy

## DOCUMENT CONTROL

<b>Document Title:</b>	Data Protection and Privacy Policy
<b>Author:</b>	Information Management
<b>Status:</b>	Approved v1
<b>Distribution:</b>	WCC, Public

## Revision History

Version	Originator	Date	Changes
1.0	Corporate Information Manager	25/11/2010	Final approved version

## Approvals

This document requires the following approvals before release,

Title/role
Strategic Director – Customers, Workforce and Governance and Senior Information Risk Owner
WCC Information Governance Steering Group

## Contents

1. Introduction.....	3
2. Scope .....	3
3. Policy requirements .....	3
4. Roles and responsibilities .....	6
5. Data protection breaches.....	6

# **Data Protection and Privacy Policy**

## **1. Introduction**

- 1.1 The Data Protection Act requires Warwickshire County Council to handle personal information relating to living identifiable individuals in a safe, responsible and secure manner. This policy sets out Warwickshire County Council's requirements regarding the appropriate and responsible use of personal information. It is underpinned by a number of related policies, codes of practice and guidelines.
- 1.2 The Data Protection Act and other legal requirements governing the use of personal information attempt to strike a balance between the privacy rights of individuals and the legitimate interests of other parties who need to access that personal information for specified purposes. The council deals with a huge amount of individuals' personal information every day, in all sorts of formats, much of which is very private. The council expects everyone who works on its behalf to recognise their responsibility for treating personal information with the care and respect it deserves.
- 1.3 The effect of a data protection breach can be very distressing and damaging to the individual concerned, and can also be damaging for the party responsible for the breach. The law does not create unreasonable barriers to the use of personal information. What the law does do is to create significant sanctions against individuals and organisations for unfair, unlawful, disproportionate, or reckless use of personal data.

## **2. Scope**

- 2.1 This policy applies to:
  - all employees
  - all workers who are not employees (e.g. individuals supplied through an agency or other company or partner or subsidiary organisations, contractors, individuals seconded to the Council or otherwise engaged on County Council business)
  - all volunteers and any individuals on work experience at the County Council
  - all Councillors.
- 2.2 Any reference in this document to "employee" is deemed to be a reference to any of the above.

## **3. Policy requirements**

- 3.1 There are a number of requirements under this policy:
  - The council's Data Protection and Privacy Commitment
  - The Data Protection Act Principles
  - The council's other policies and guidance on the use of personal information, which are part of the Council's Information Governance Framework.

### **Data Protection and Privacy Commitment**

- 3.2 The council has made a Data Protection and Privacy Commitment which explains the approach taken by the council to comply with the Data Protection Act 1998, the Human Rights Act 1998, the duty of confidence and other

# Data Protection and Privacy Policy

legislation and best practice relating to the use of personal information. Everyone to whom this policy applies is required to meet the Data Protection Commitment.

## 3.3 The Data Protection and Privacy Commitment is as follows:

The Council will seek to meet its obligations in law and in spirit and achieve an appropriate balance between the Council's resources, confidentiality, other people's rights to privacy and the purposes for which the information is held by:-

- being transparent and fair in the way that the Council meets its legal obligations recognising the rights to privacy of individuals
- valuing the personal information entrusted to us and make sure we respect that trust
- consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems or new ways of working
- ensuring information held about individuals is accurate, relevant and subject to clear archiving and destruction policies
- ensuring that there are proper security measures in place to protect the confidentiality of individuals
- obtaining written, informed consent to collect, share and process personal information wherever reasonably practicable
- informing citizens what information we collect and share about them
- ensuring that personal information is used in ways which are proportionate and not excessive or unreasonable
- facilitating access to information where this does not prejudice the purpose for which the information is held or infringe rights to privacy
- maintaining up to date data protection registration with the Information Commissioner
- treating people justly and fairly whatever their age, religion or belief, disability, gender, sexual orientation or ethnicity when dealing with requests for information
- raising awareness through effective staff training and induction
- treating it as a disciplinary matter if employees misuse or don't look after personal information properly
- setting out clear procedures for responding to requests for information
- setting out clear procedures for making a complaint and ensuring a prompt response.

## The Data Protection Act Principles

## 3.4 The Data Protection Act sets out eight Data Protection Principles to secure the responsible use of personal information. Some guidance on the Principles and the terms used by the Act can be found in the Glossary.

# Data Protection and Privacy Policy

- 3.5 All employees must comply with the eight Data Protection Principles and the Council's policies and guidelines that underpin those Principles, which state that an individual's personal information should be:
- (1) Processed fairly and lawfully
  - (2) Obtained for one or more specified and lawful purposes, and will only be further processed in compatible manner
  - (3) Adequate, relevant and not excessive for the purposes
  - (4) Accurate and where necessary kept up to date
  - (5) Not kept for longer than is necessary for the purposes
  - (6) Processed in line with the individual's rights
  - (7) Appropriate technical and organisation measures to keep secure
  - (8) Not transferred to other countries outside the European Economic Area without adequate protection.
- 3.6 The Data Protection Principles also make it clear that personal information which is particularly sensitive (for example, information which relates to an individual's racial or ethnic origin, health, religion or belief, sexual life, trade union membership, political affiliations or criminal offences or proceedings) must be treated with special care. Information which is subject to a "duty of confidence" must also be treated with special care.

## Information Governance Framework policies and guidance

- 3.7 To help the council and its employees comply with the Data Protection and Privacy Commitment and the Data Protection Principles, the council has developed a number of other policies and guidance relating to personal information, data protection and privacy. These form part of the council's "Information Governance Framework", which sets out responsibilities for lawful and responsible use of information generally. These will be published on the council's website and staff Intranet and include:
- Information Responsibilities for All Staff
  - Information Security Policies
  - Privacy Notices and Standards
  - Access to Information Policies
  - Warwickshire Information Sharing Charter
  - Information sharing protocols for service specific areas
  - Codes of Conduct for Members, employees and employer
  - Procedures on use of CCTV and use of photographic images
  - Policies and guidance issued for service specific areas (e.g. confidentiality of customers' records in social care settings)
  - Any other instructions, guidance and controls issued by managers from time to time.

# **Data Protection and Privacy Policy**

## **4. Roles and responsibilities**

- 4.1 Every employee and other person to whom this policy applies is responsible for the appropriate use and protection of personal information which is in their possession or use. Everyone is also responsible for familiarising themselves with their obligations under this policy and related ones, for ensuring their own compliance and for seeking guidance where they need it.
- 4.2. Managers are responsible for controls that ensure compliance with this policy. This will include induction of new staff, implementation of new procedures and systems and providing appropriate communications and awareness-raising of the policy requirements.
- 4.3 The council will designate a Data Protection Officer and each directorate will also have a nominated coordinator who has responsibility for coordinating and supporting staff on data protection and privacy policy and procedures within their directorate.
- 4.3 Information Asset Owners (normally Heads of Service) are responsible for the information assets under their control including personal information. This includes identification, access, security, and privacy of personal information. They are responsible for making sure employees who access or handle personal information are suitably trained in data protection and privacy in order to understand their obligations under this policy. They will incorporate an assessment of data protection and privacy risk into their risk management arrangements.
- 4.4 The council's Chief Executive and Strategic Directors are responsible for ensuring a co-ordinated response from the council and its employees to this policy and for keeping under review the council's approach to personal information, data protection and privacy.
- 4.5 The council's Cabinet are responsible for ensuring that sufficient resources are made available to support the council and its employees in meeting the obligations under this policy.
- 4.6 The council's Monitoring Officer shall be responsible for liaison with the Information Commissioner over data protection notifications and other issues as appropriate.

## **5. Data protection breaches**

- 5.1 Any incident that could or does lead to loss, disclosure or temporary exposure of personal information must be reported to Information Security as stated by the WCC Incident Management policy and procedures.
- 5.2 The council has procedures for investigating data protection and privacy breaches and all those affected will be expected to co-operate with any such investigation.
- 5.3 Serious data protection breaches will be reported to the Information Commissioner by the council's Monitoring Officer.
- 5.4 Disregard for the council's data protection and related policies by employees may be regarded as misconduct to which the council's Dismissal and Disciplinary Procedure applies and a serious breach of any policy may be treated as gross misconduct and may lead to dismissal. In the case of contractors, representatives, workers and volunteers, this may be grounds for termination of that relationship with the council.