

# Data Protection Policy - Cambridgeshire County Council

## Statement of Commitment

In order to undertake its statutory obligations effectively, deliver services and meet customer requirements, Cambridgeshire County Council needs to collect, use and retain information, much of which is confidential. Such information may be about:

- Our service users.
- Our employees or their families.
- Members of the public.
- Members of the Council.
- Business partners.
- Other local authorities or public bodies.

We regard the lawful and correct treatment of personal data by Cambridgeshire County Council (the Council) as very important for successful operations, and to maintain the confidence of our stakeholders.

To this end, the Council will ensure compliance, in all its functions, with the Data Protection Act 1998 (the DPA 1998) and other relevant legislation.

## Compliance with the Principles

The Principles of the DPA 1998 state that personal information must be:

- Processed **fairly and lawfully** and, in particular, shall not be processed unless specific conditions (detailed in the DPA 1998) are met;
- Obtained only for one or more **specified and lawful purposes**, and shall not be further processed in any manner incompatible with that purpose/those purposes;
- **Adequate, relevant and not excessive** in relation to the purpose or purposes for which it is processed;
- **Accurate** and, where necessary, kept up to date;
- **Kept only for as long as is necessary** for that purpose or those purposes;
- **Processed in accordance with the rights of data subjects** under the DPA 1998;
- **Kept secure** and appropriate technical and organisational measures taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data; and,
- Transferred only to a country or territory outside the European Economic Area (EEA) that ensures an **adequate level of protection** for the rights and freedoms of data subjects in relation to the processing of personal data.

In order to comply with these principles the Council will:

- Observe and comply with the conditions regarding the **fair collection and use** of personal data;

- **Specify the purpose** for which personal data is used;
- Only collect and process appropriate personal data **to the extent that it is needed** to fulfil operational needs or to comply with legal requirements;
- Ensure the **quality** of data used;
- Apply **retention schedules** to determine the length of time information is held and dispose of information securely when it has reached its disposal date;
- Ensure that the **rights of individuals** about whom the data is held can be fully exercised under the DPA 1998;
- Take appropriate **security measures** to safeguard personal information; and,
- Ensure that **personal data is not transferred** outside the country without suitable safeguards.

In addition the Council will ensure that:

- There is an **appointed officer** with responsibility for Data Protection.
- Employee and Member **training needs** are identified and training provided, where appropriate, to ensure that those managing and handling personal information understand their responsibility to follow good data protection practice.
- A regular **review and audit of the use of personal data** is undertaken to ensure compliance with the DPA 1998.
- **Methods of handling data are clearly described** and queries about the handling of personal information are dealt with promptly.
- If **new services or processes** are being introduced which affect what personal information will be collected, how it is used and managed and who will do this, a short **Privacy Impact Assessment (PIA)** should be conducted to identify any Information Governance issues which need to be addressed as part of the project. The Information Governance Team should be notified of the need for this as early as possible in the project.

### **Information Sharing**

'Information sharing' is the sharing of sensitive and/or personal information in a closed way, between or within organisations as part of integrated working or service delivery. The Council encourages lawful information sharing undertaken in line with best practice, both within the Council and with relevant third parties. It is a member of the Cambridgeshire Information Sharing Framework (the Framework), whose purpose is to facilitate more effective information sharing across the County.

In instances of sharing, in order to comply with the Data Protection Act and other relevant legislation, the Council will give consideration to the following before sharing personal and/or sensitive information with third parties:

- whether the Council has the **power to share** the information (considering the Data Protection Act and other relevant legislation including the Children Act 2004);
- whether the sharing can be **justified**;
- whether the sharing is to be carried out on an **ad hoc** or **systematic** basis and therefore whether an **information sharing agreement** should be created; and
- how to ensure the **security of information being shared**.

In particular, the Council will ensure that all obligations regarding information sharing in safeguarding situations are met, regardless of the existence of any agreements.

In line with the Framework, where personal and/or sensitive information is being shared systematically between organisations working together in a partnership or subcontracting arrangement, the involved services will ensure that information sharing agreement or contractual agreement is in place.

All information sharing agreements agreed or revised after March 2012 must be signed off by the relevant Information Asset Owner(s) who are accountable for the information that is being shared and by the Information Governance Manager before the sharing is undertaken or as soon as practical thereafter.

A log of Information Sharing Agreements involving Council services shall be maintained by the Information Governance Team.

### **Rights of the Individual**

Individuals will be informed about what we will do with their personal information using appropriate tools including 'fair processing notices'.

Upon receipt of a written request by an individual to obtain a copy of the information the Council holds about them (a Subject Access Request), and following verification of the requester's identity, the Council will provide any information that is held about that individual in a form that is clear, and with all references explained in accordance with the DPA 1998 (subject to exemptions provided for by the Act and other relevant legislation).

Records (both current and closed) must be organised and managed in such a way that services can identify and supply the whole record set relevant to an individual's request in a timely fashion. To support this, records relating to individual case files must be stored in the case file and not, for example, in individual email accounts or My Documents.

The statutory time limit for responding to a Subject Access Request under the Data Protection Act is 40 calendar days.

The Council will respect any request made by individuals to opt out of any records held that are not necessary for the running of the Council's services and performance of its statutory duties.

If an individual identifies errors of fact in the information the Council holds about them, these must be verified and rectified as soon as possible and confirmation sent to the individual.

A log of Subject Access Requests is maintained by Information Governance. This team should be notified at [data.protection@cambridgeshire.gov.uk](mailto:data.protection@cambridgeshire.gov.uk) where an individual has requested access to the information the Council holds about them.

### **Compliance**

This Policy applies to all Council employees (except those directly employed by schools, where parallel arrangements apply), Council Members and all people or organisations acting on behalf of the Council.

Each Director shall ensure compliance with the policy. If any persons acting on the Council's behalf are found to knowingly or recklessly breach the Council's Data Protection Policy, appropriate disciplinary and/or legal action shall be taken.

If personal and/or sensitive information is lost or compromised Business Support Helpdesk must be contacted straightaway in accordance with the Information Security Incident Policy.

### **Further information**

**Senior Information Risk Owner** – Sue Grace  
01223 699248, [sue.grace@cambridgeshire.gov.uk](mailto:sue.grace@cambridgeshire.gov.uk)

**Corporate Information Manager** – Dan Horrex  
01223 728416, [dan.horrex@cambridgeshire.gov.uk](mailto:dan.horrex@cambridgeshire.gov.uk)

**Information Governance Manager** – Catherine Preston  
01223 699137, [data.protection@cambridgeshire.gov.uk](mailto:data.protection@cambridgeshire.gov.uk)