Hampshire County Council

Hampshire County Council Data Protection Policy

Version	Status	Date	Next Review Date
V2.0	Published	June 2020	June 2021

Contents

1. POLICY STATEMENT

1.1. Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our customers, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2. County Council employees are obliged to comply with this policy when processing personal data on our behalf.

2. ABOUT THIS POLICY

2.1. The types of personal data that the County Council may be required to handle include information about current, past and prospective customers and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (together referred to as the Data Protection Legislation).

2.2. This policy, along with the County Council's General Privacy Notice and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources correctly and securely and in accordance with the Data Protection Legislation.

2.3. This policy has been approved by the County Council's Risk Management Board. It sets out rules on data protection and the conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.4. The Data Protection Officer is responsible for monitoring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Officer at data.protection@hants.gov.uk.

2.5. The Data Protection Officer will be responsible for completing the annual notification to the ICO and advising them of any updates to the register within 21 days.

3. DEFINITION OF DATA PROTECTION TERMS

3.1. **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.2. **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, a unique reference number, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.3. **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with GDPR. The County Council is in most cases the data controller of personal data it collects or uses in its day to day business and in providing services.

3.4. **Data processors** are any person or organisation that processes personal data on our behalf and on our instructions. Employees of data controllers are not data processors, but it includes suppliers, providers and contractors which handle personal data on the County Council's behalf.

3.5. **Processing** is any activity that involves use of the data. It includes obtaining, recording or storing data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, viewing, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.6. **Special Category Data** is information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and genetic data, biometric data (for the purpose of uniquely identifying an individual), data concerning health, an individual's sex life or sexual orientation. Special Category Data can only be processed under strict conditions. Personal Data relating to criminal convictions and offences is subject to additional requirements and should be handled in a similar way to Special Category Data.

3.7. **Third Party** - Any individual/organisation other than the data subject, the data controller or its processors.

4. RESPONSIBILITIES UNDER THE GENERAL DATA PROTECTION REGULATION (GDPR)

4.1. The County Council is a Data Controller of personal information it processes on its own behalf it is also a Processor of information for other organisations. The County Council maintains records of all its processing activities and keeps records of the lawful basis for processing categories of data.

4.2. The Data Protection Officer is responsible for monitoring compliance with GDPR and with this policy and may assign officers to support this process.

4.3. The Corporate Management Team, through the Risk Management Board, is responsible for developing and encouraging good information handling practice within the County Council.

4.4. Compliance with Data Protection Legislation is the responsibility of everybody who processes personal information.

5. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the six principles relating to processing of personal data in the GDPR. These provide that personal data must be:

5.1. **Processed lawfully, fairly and in a transparent manner** in relation to the data subject ('lawfulness, fairness and transparency').
For personal data to be processed lawfully, it must be processed on the basis of one of the lawful bases set out in the GDPR. Relevant examples of these bases include, processing that is necessary:

- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the County Council
- for the performance of a contract to which the data subject is party
- for compliance with a legal duty

- the data subject has given consent for the data to be processed for a specific purpose(s).

When special category data is being processed, additional conditions must be met. When processing personal data as a data controller in the course of our business, we will ensure that those requirements are met.

Personal data is processed in a transparent manner by providing data subjects with privacy notices. These are supplied to the data subject directly and/or are available on the County Council's website.

5.2. **Collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes.

We will only process personal data for the specific purpose(s) set out in the County Council's records and privacy notices or for any other purposes specifically permitted by the legislation. We will notify those purposes to the data subject when we first collect the personal data or as soon as possible thereafter.

5.3. **Adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed ('data minimisation').

Personal data, which is not necessary for the purpose for which it is obtained, should not be collected. If personal data is given or obtained which is excessive for the purpose, it should be deleted or destroyed without delay.

5.4. **Accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

Personal Data, which is kept for a long time, must be reviewed and updated as necessary. No personal data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that personal data held by the County Council is accurate and up to date. Individuals should notify the County Council of any changes in circumstance or of factual details e,g, change of name or contact details to enable personal records to be updated accordingly. It is the responsibility of the County Council to ensure that any notification regarding change of circumstances is noted and acted upon.

5.5. **Kept in a form which permits identification of data subjects for no longer than is necessary** for the purposes for which the personal data are processed ('storage limitation').

We will not keep personal data longer than is necessary for the purpose(s) for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required. Data will be kept in accordance with the County Council's retention periods which ensure that data is not kept for longer than necessary.

On occasion, personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR.

5.6. **Processed in a manner that ensures appropriate security of the personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'). The County Council has appropriate security measures in place to protect data, details of which are provided below.

6. NOTIFYING DATA SUBJECTS

6.1. If we collect personal data directly from data subjects, we will inform them through our Privacy Notices about:

(a) The purpose or purposes for which we intend to process that personal data.

(b) The legal basis for processing.

(c) The types of third parties, if any, with which we will share or to which we will disclose that personal data.

(d) The length of time that we will retain the data.

(e) The means, if any, with which data subjects can limit our use and disclosure of their personal data.

(f) Their right to make a complaint to the ICO.

6.2. If we receive personal data about a data subject from other sources, we will provide the data subject with this information within the required timescales.

6.3. We will also inform data subjects whose personal data we process that we are the data controller with regard to that data, and the contact details of our Data Protection Officer.

7. DATA SECURITY

7.1. We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or destruction of, personal data.

7.2. We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

7.3. Personal data will only be transferred to a data processor who has provided sufficient guarantees to implement appropriate technical and organisational measures that will comply with the Data Protection legislation and ensure that data subjects rights are protected and that these requirements are governed by a contract or other legally binding agreement.

7.4. We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) Confidentiality means that only people who are authorised to use the personal data should access it.

(b) Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users should be able to access the personal data if they need it for authorised purposes.

7.5. Security procedures include:

(a) Entry controls. Any stranger seen in entry-controlled areas will be reported.

(b) Secure lockable desks and cupboards. Desks and cupboards will be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(c) Methods of disposal. Paper documents will be shredded and securely disposed of. Digital storage devices will be physically destroyed when they are no longer required.

(d) Equipment. County Council employees will ensure that the personal data they use in the course of their work is only shared with those who are entitled to see it.

(e) IT Security. The County Council will maintain up to date firewalls, patching and other IT security measures.

7.6. Training for staff includes:

(a) Mandatory training for all staff on Data Protection, with refresher training

(b) Training for specialist Data Protection staff, including those who handle Subject Access Requests

(c) Training about data security is provided for systems where required.

7.7. Governance and assurance procedures include:

(a) An Information Governance framework overseen by the Data Protection Officer

(b) The appointment of a Senior Information Risk Officer, with cross-organisational oversight provided by the County Council's Risk Management Board

(c) The regular audit of the County Council's Information Management processes and procedures.

8. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

8.1. We will only disclose or share a data subject's personal data where we are legally permitted to do so, in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

8.2. The County Council will enter into Data Sharing Agreements with other data controllers where appropriate.

9. INDIVIDUAL'S RIGHTS UNDER THE GDPR

9.1. Individuals have a number of rights under the GDPR including the right to:

- ask the County Council if it holds personal information about them
- ask what it is used for
- be given a copy of the information
- be given details about the purposes for which the County Council uses the information and of other organisations or persons to whom it is disclosed.

- ask for incorrect data to be corrected.
- be given a copy of the information with any unintelligible terms explained
- be given an explanation as to how any automated decisions taken about them have been made.
- ask that information about them is erased ("right to be forgotten")
- ask the County Council not to use personal information:
  - for direct marketing,
  - to make decisions which significantly affect the individual, based solely on the automatic processing of the data.

9.2. Some of these rights are subject to conditions which are set out in the GDPR. If the County Council is unable to respond to a request, it will outline the reasons for its decision clearly.

10. DEALING WITH DATA SUBJECT REQUESTS

10.1. The County Council has provided application forms on its website to assist data subjects to make a request regarding their personal data..

10.2. Data subjects can make a request for information we hold about them. We recommend that these requests are made in writing where possible. Employees who receive a request should forward it to the County Council's Information Governance Team.

10.3. Any individual who wishes to exercise their data subject rights should on request provide satisfactory proof of identity and sufficient information to enable the data to be located.

10.4. Subject to satisfactory completion of the 10.3 above, the County Council should respond within one month and in accordance with any relevant exemptions specified in the legislation.

11. DEALING WITH A POTENTIAL DATA PROTECTION BREACH

11.1. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

11.2. The County Council has a process for managing data protection incidents. As part of the process employees are required to follow guidelines on reporting a potential data protection breach including completing a data incident reporting form.

12. DATA PROTECTION IMPACT ASSESSMENTS

12.1. The County Council must carry out a Data Protection Impact Assessment (DPIA) when processing personal data is likely to result in a high risk to the rights and freedoms of natural persons. This process identifies and mitigates any potential risks to the rights and freedoms of the data subject prior to new data processing being undertaken.

12.2. The County Council has a procedure for employees to follow which includes guidance on assessing whether a DPIA is required.

13. RETENTION AND DISPOSAL OF DATA

13.1. The County Council discourages the retention of personal data for longer than they are required. Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion).

13.2. The County Council maintains Retention Schedules that are specific and relevant to specific types of information and the services they relate to. These outline the appropriate periods for retention. The Retention Schedules are kept under review and updated as required. On occasion, the County Council will retain data outside the retention period for example where the County Council is legally obliged to do so (e.g. Independent Inquiry into Child Sexual Abuse (IICSA)).

14. USE OF CCTV

14.1. The County Council's use of CCTV is regulated by the Surveillance Camera Commissioner. The County Council complies with the Surveillance Camera Code of Practice and the ICO Code of Practice, supplemented by local policy and guidance.

15. FREEDOM OF INFORMATION ACT 2000

15.1. The Freedom of Information Act 2000 (FOIA) allows public access to all types of information held by public authorities. Requests for personal information will be dealt with under the Data Protection Legislation.