Data Protection Policy for Staff

Version	Status	Date	Next Review Date
V2.4	Published	February 2023	January 2024

Contents

1	Policy Statement	1
2	Scope	2
3	What is Personal Data?	2
4	Processing Data	3
5	Data Protection Principles	4
6	County Council Obligations	5
7	Employee Obligations	5
8	Definition of Misuse or Unacceptable Behaviour	6
9	Individual Rights Under the Data Protection Legislation	7
10	Links to Other Policies	7
Appendix 1	Privacy Statement for Staff	8

1. **Policy Statement**

1.1. The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (together known as the Data Protection Legislation) regulate the way in which personal data about a member of staff is held and used.

1.2. The general aim of the Data Protection Legislation is to ensure that where personal data is held, the data is adequate, relevant and not excessive. The Data Protection Legislation also ensures that staff are able to access and review the contents of any files held on them.

1.3. This policy applies to the personal data of job applicants, employees (including employees who are working out their notice period, and seconded employees), workers, contractors, volunteers, interns, apprentices. These will be collectively referred to as "staff".

1.4. Throughout their employment or position and for as long a period as is necessary following the termination of employment or position, the County Council will need to keep

information for purposes connected with a member of staff's employment. The County Council will also hold information to ensure that required services are provided in an efficient, effective manner.

1.5. The County Council has provided a Privacy Notice for Staff which sets out details about how it processes personal information about staff that, the purpose, lawful basis for processing, and how it shares and retains this information. The Privacy Notice for Staff is appended to this Policy.

1.6. The County Council endorses and adheres to the Principles Relating to Processing of Personal Data set out in Article 5 of the UK GDPR and requires all staff to comply with the Data Protection Legislation in relation to all personal data held by the County Council including the personal data about staff.

1.7. Staff should at all times value the right to privacy of the people about whom information is held and should manage personal information professionally. It is each member of staff's responsibility to ensure that personal data they have access to in the course of their employment or position remains confidential and secure. The aim of this document is to provide staff with information relating to the County Council's obligations in relation to data protection and guidance on matters such as how staff are expected to handle personal data under the Data Protection Legislation. More information can be found in the Safe Information Handling Policy on the Data Protection intranet pages.

1.8. Failure to comply with this Guidance, the associated County Council's policies outlined in sections 9 and 10 below and the principles set out in the Data Protection Legislation will be regarded as misconduct and will be dealt with in accordance with the County Council's Managing Misconduct Policy. Misuse and unauthorised disclosure of personal data can lead to prosecution of individuals.

2. Scope

2.1. This document applies to all employees.

2.2. The principles in this document also apply to:

- Former employees
- Seconded employees
- Job applicants (successful and unsuccessful)
- Former job applicants
- Agency workers
- Casual workers
- Contract workers
- Volunteers
- Trainees / work placement students

2.3. For the purposes of this document, these categories of individuals will be referred to collectively as "staff".

3. What is personal data?

3.1. ‘Personal data’ means any information relating to an identified or identifiable individual (‘data subject’). This means someone who can be identified, directly or indirectly, by an identifier such as a name, an identification number, location data or an online identifier.

3.2. Personal data held about staff will include:

- Name and or address/postcode
- Personnel number
- Photographs
- CCTV footage

3.3. These records may include:

- information gathered about a member of staff and any references obtained during recruitment
- details of terms of employment
- payroll, tax and National Insurance information
- performance information
- details of grade and job duties
- health records
- absence records, including holiday records and self-certification forms
- details of any disciplinary investigations and proceedings
- training records, requests and associated details
- contact names and addresses, including personal email addresses
- correspondence with the Council and other information provided to the Council.

3.4. Some personal data is also classed as “special category data” and attracts a higher level of protection under the UK GDPR. This more sensitive personal data is information relating to:

- Race or ethnic origin
- Political opinions
- Religion or philosophical belief
- Trade union membership
- Health (including Disability)
- Sexual orientation
- Gender identity
- Genetic data or Biometric data

3.5. Criminal offence data is dealt with separately in the Data Protection Legislation but will be treated the same as special category data.

4. Processing data

4.1. For the purposes of the UK GDPR, the term 'processing' includes the initial collection of personal data, the holding, use and viewing of such data, as well as access, sharing and disclosure, through to final destruction.

4.2. If the County Council intends to process personal data it must be processed fairly and lawfully and must comply with the conditions for processing set out in the UK GDPR. The County Council must ensure that there is a lawful basis for processing.

4.3 The provisions of the Data Protection Legislation permit the County Council to process a member of staff's personal data and special category data. The County Council will only process personal data and special category data where permitted by law, for example, where processing is necessary for the purposes for the performance of a contract (e.g. the employment contract) and in relation to special category data, processing is necessary for the purposes of carrying out obligations in the field of employment. If appropriate, special category data will be processed with the explicit consent of staff.

4.4 In relation to referrals to the County Council's Occupational Health Service, consent will be obtained before data is processed. However, other lawful bases for processing may also apply to work undertaken by Occupational Health.

5. Data Protection Principles

5.1. The UK GDPR contains a series of principles which govern the manner in which personal data is processed. The principles require that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) 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');

(e) 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; 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) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) 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').

6. County Council obligations

6.1. As part of the County Council's commitment to maintaining public confidence and in order to comply with the Accountability principle under Article 5(2), the County Council will:

- Ensure there is a designated Data Protection Officer.
- Ensure that staff handling personal data understand that they are contractually and/or professionally responsible for compliance with the data protection policy and are appropriately trained and supervised for these purposes.
- Provide appropriate training on data protection for staff commensurate with their duties.
- Ensure that data subject rights can be exercised and are dealt with in accordance with Data Protection Legislation.
- Conduct regular reviews, evaluations and audits of the way personal data is managed within the County Council.

6.2. The County Council's Data Protection Officer can be contacted at data.protection@hants.gov.uk

7. Staff obligations

7.1. Staff must work within the requirements of the Data Protection Legislation at all times and:

- ensure that personal data is only disclosed to those who are entitled to receive it
- ensure that they understand any departmental guidelines or operational procedures on data disclosure e.g. adopted practice in establishing identity of telephone callers
- take care to ensure that data stored both on paper and electronically is accurate and up to date
- ensure that they are aware of their Section / Service security procedures in place for protecting data and follow those procedures
- ensure that they follow the County Council's policies and procedures in respect of data protection and the safe handling of information
- ensure that they follow the County Council's Policy for dealing with Potential Data Protection Incidents (found on the Data Protection intranet pages) where relevant

- ensure that their behaviour in respect to handling information does not constitute misuse or unacceptable behaviour as defined in section 8

7.2. Staff MUST NOT:

- Disclose confidential information without authorisation
- Use any personal data held by the County Council for their own personal use.

7.3. Staff MAY:

- Handle and use personal data where it is necessary to carry out their work
- Transfer personal data within the County Council between departments provided that one or more of the following apply:
  - permission from supervisor is obtained
  - any Information Sharing Agreement or other processes or rules in place regarding the transfer of personal data are followed
  - data is used for the purposes for which it was obtained
  - consent of the data subject is obtained

7.4. If a member of staff is in any doubt about whether to disclose information, advice should be sought from the Departmental Data Protection Coordinator. Where required, the Departmental Coordinator will seek advice from Legal Services.

8. Definition of Misuse or Unacceptable Behaviour

8.1. The standards by which the County Council expects that its information should be treated are contained in the County Council's Safe Information Handling Policy and Corporate Acceptable Use Policy.

8.2. Staff are personally responsible at all times for the personal and/or sensitive information (i.e. special category data), in whatever format, in their care. They must safeguard the security of personal and/or sensitive information for which they are responsible or which they access in order to carry out their work.

8.3. The County Council will enforce this policy through its Managing Misconduct Policy. Breaches of this policy could lead to disciplinary action and sanctions up to and including dismissal, depending on the breach and its impact.

8.4. Examples of misuse or unacceptable behaviour include:

1. Inappropriately or without authorisation, removing personal, special category, sensitive, confidential or high risk business information from the organisation's premises, IT systems or environment where it is usually stored;

2. Loss or inappropriate sharing or dissemination of personal, special category, sensitive, confidential or high risk business information from the organisation's premises, IT systems or environment in which it is usually stored;

3. Inappropriately or without authorisation, accessing personal, special category, sensitive, confidential or high risk business information that they are not entitled to for the purposes of their role;

4. Failing to report a possible/potential data protection breach or failing to assist with the investigation into such a potential data protection breach;

5. Through action or inaction allowing, permitting or causing staff under their control to operate in such a manner as any of the above occurs.

9. Individual's Rights Under the Data Protection Legislation

9.1. Section 2 sets out a list of individuals to whom this policy applies, the key principle being both current staff and individuals not employed by the County Council are entitled to request certain information under the Data Protection Legislation. These individuals have the right:

- To ask the County Council if it has collected or is using personal information about them
- To ask what it is used for
- To be given a copy of the information (subject to any relevant fees and exemptions) ("subject access request")
- To 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
- To be given an explanation as to how any solely automated decisions taken about them have been made.
- To ask for incorrect data to be corrected
- To ask that information about them is erased ("right to be forgotten")
- The right to restrict processing in some circumstances
- The right to portability (if relevant)
- To ask the County Council not to use personal information in certain circumstances, including:
    - for profiling in some circumstances, including direct marketing;
    - to make decisions which significantly affect the individual, based solely on the automatic processing of the data.

9.2. In most cases, these rights are not absolute. If the County Council refuses such a request, it will provide the legal reasons for its decision.

9.3. As referenced above, individuals may request access to any of their personal data held by the County Council by making a subject access request. There are some limited circumstances in which personal data relating to the applicant may be withheld. Examples of this include repeat access requests, confidential references, and third party information.

10. Links to other Policies

10.1. This Policy should be read in conjunction with other relevant County Council policies, including the General Privacy Notice, Safe Information Handling Policy, Corporate Acceptable Use Policy, Managing Misconduct Policy, Code of Conduct, IT Security Guide and Policy for dealing with Potential Data Protection Incidents.