Human Resources **Working at Essex County Council**

Data protection in employment policy

Essex County Council

Contents

The aim of this policy

This policy sets out the Council's responsibilities as an employer under the Data Protection Act (DPA) 1998 and provides guidance on the maintenance of and access to employment records, in accordance with the provisions of this Act. The policy has been updated to reflect the changes which came into effect in October 2001 in relation to manual data and the rights of individuals to access data held on them, both manual and computerised.

Data Protection in Employment Policy

1. The Council's responsibilities

The Council recognises and accepts its responsibilities as a data controller under the Data Protection Act 1998.
The Council continues to notify the Data Protection Commissioner of the personal data it processes and to comply with the eight data protection principles set out in the Act. In summary they require personal data to:

- be processed fairly and lawfully;
- be obtained only for specified and lawful purposes;
- be adequate, relevant and not excessive in relation to the purposes for which it is processed;
- be accurate and kept up to date;
- be kept for no longer than is necessary;
- be processed in accordance with the rights of data subjects under the Act;
- be subject to appropriate measures to protect unauthorised or unlawful processing;
- have certain restrictions for any transfer outside the European Economic Area.

2. Employee Rights and Responsibilities

2.1 Employee Rights

With effect from October 2001, all workers, both current and former (i.e. permanent and temporary employees, casual workers, contract workers and agency workers) and job applicants (successful and unsuccessful) have the following rights:

i. to access manual, as well as automated records where such information is kept in a structured way and where this information is not covered by an exemption, or other circumstance prohibiting disclosure – see paragraph 9.

ii. to be supplied, following a written request (including by e-mail), with a copy of the data that concerns them, to be told why the data is being kept and be given information about any person(s) to whom that data has, or may be disclosed.

iii. to seek to prevent processing of the data which is likely to cause them damage or distress.

iv. to object to solely automated decision taking e.g. recruitment decisions made by automated means only.

v. to take action to have inaccurate personal data corrected or erased.

vi. to seek compensation if they feel they have suffered damage by any breach of the DPA.

The process for accessing personal information is set out in paragraph 10 below.

2.2 Employee responsibilities

All employees have an obligation to safeguard the personal data of others, both automated and manual, which they handle in the course of their day to day duties. All employees are required to comply both with this policy and to co-operate in measures introduced by the Council to implement them. Any breach of the principles of this policy could result in disciplinary action and any breach of the Data Protection Act could constitute a criminal offence.

Under the Gender Recognition Act 2004 it is also a criminal offence to disclose that someone has (or has applied for) a gender recognition certificate.

3. Employment data covered by the act

All automated personal data is covered by the Act. This includes:

- Computerised records on data bases.
- Images or documents on computerised systems.
- Images or documents held on microfiche.
- CCTV (where enough information is provided to locate images relevant to the individual).
- Back-up data (if specifically requested).

Manual data is also covered by the Act where it is held, or intended to be held, in a 'relevant filing system'. The definition of this is broad and covers, essentially, any set of information about an employee (s) in which it is easy to find a piece of information about that employee.

The following list indicates the nature of information which is, or may be held by the Council about workers. Such information is covered by the DPA and therefore, if an employee requests disclosure of information held on them, this should include the following, unless agreed otherwise with the employee (see paragraphs 9.1 and 9.2). It is not necessary to obtain the prior consent of employees to keep this information.

- Payroll and tax information.
- Job application forms.
- Interview notes.
- Annual leave records.
- Parental leave/special leave records.
- 'my performance' documentation.
- 'Supervision' notes.
- Records relating to disciplinary, grievance or capability processes, including information held on the Council's 'List and Indices' of people considered unsuitable to work with children or vulnerable people, or of people who have left the Council's service for, e.g. reasons relating to disciplinary action.
- Records relating to training, promotion, transfers.
- Records relating to injuries or accidents at work.
- Any summarised records of service.
- E-mails about incidents/expressions of opinions involving named workers, or where the worker is the subject of the e-mail, including where such e-mails have been deleted.
- Confidential management 'notes' or memos, hand-written or computerised, about an individual which are kept, or intended to be kept on a structured file.
- Records relating to 'interviews e.g. absence review meetings, held with the employee.

Note: this list is not exhaustive and there may well be other records relevant to disclosure of information requests.

4. Sensitive Personal Data

The DPA sets out a series of conditions, at least one of which has to be met before 'sensitive' personal data can be collected, stored, used, disclosed or processed. Sensitive data is defined as that relating to:

- Racial or ethnic origin.
- Political opinions.
- Religious beliefs or other beliefs of a similar nature.
- Trade union membership.
- Physical or mental health or condition.
- Sexual life.

- Commission or alleged commission of a criminal offence.
- Proceedings for an offence or alleged criminal offence.

As far as the Council is concerned, the sensitive data held about workers and job applicants is likely to cover ethnic origin, trade union membership, physical or mental health (as part of sickness records), disability, age, gender, religion or belief, sexual orientation and issues relating to criminal offences.

Whilst individuals should know that this information is kept, it is not necessary to obtain individual consent to the keeping of this information. The DPA allows organisations to keep such information where doing so meets a 'sensitive data condition' such as enabling the organisation to fulfil another statutory duty. In this context, for example:

- diversity information, for example ethnic origin – this is covered by the Council's obligations under the Equality Act 2010;
- trade union membership – to allow deductions to be made directly from salary;
- sickness records (see below) to, for example, enable the Council to meet the requirements imposed on it by the law in relation to Statutory Sick Pay (SSP);
- disability – to enable reasonable adjustments to be made.

If, however, the Council were for example to retain information about political opinions, religious beliefs or sexual life, it would be necessary to obtain the explicit consent of the worker. Such consent should be written and recorded, and set out the nature of the data to be processed, the reason it is being kept and any other relevant information.

Example:

It might occasionally be necessary to keep specific information about religious beliefs/practice where adjustments to working patterns have been accommodated for reasons of religious observance. In such circumstances the consent of the worker should be sought on a case by case basis by requiring them to sign and date a statement acknowledging that the information is being kept.

5. Sickness records

The Data Protection Code on Employment Records distinguishes between 'absence' records and 'sickness and accident' records. Absence records, which simply record the fact of the absence, can certainly be kept without the need for individual consent. Sickness and accident records, similarly, may be kept and used in a reasonable way, without individual consent, as the keeping of such records is likely to satisfy a 'sensitive data condition'. However, where information from a worker's sickness or accident record relating to an illness or medical condition is to be disclosed, then the written consent of the employee will be needed, unless there is a legal obligation to disclose the information.

Example:

A request from another employer for information relating purely to the number of days of sickness of a prospective employee can be answered from information available on absence records and without recourse to the employee. This would be 'absence' information.

If, however, the other employer wants further information, relating to the detail of why the employee was sick, this information must not be given without the consent of the employee concerned as this would be 'sickness' information.

Note: information relating to sickness can be shared between Human Resource (HR) teams and with managers within the Council for legitimate employment purposes and as long as such information is used in a reasonable way. For example, in an ill-health redeployment situation it may be necessary to share the reason for sickness with the manager of the new work area so that, for example, any necessary adjustments can be made.

Notwithstanding the above, the Council's Return to Work form includes the following declaration to be signed by the employee: 'I acknowledge that the personal information provided will be dealt with in a confidential manner and only for the purposes of managing attendance'.

6. Retention Periods for Employment Information

Guide 1 sets out recommended retention times for the information set out in paragraph 4 above. Whilst listed separately, much of the information will be kept on individual personal files, where held by Corporate Operations, Payroll, and therefore retained for 7 years following the end of employment, in accordance with the retention time for personal files.

Note: it will be the responsibility of Corporate Operations, Payroll who will be sending the information to Records Management to flag up the destruction time for the information. In the case of personal files, whilst the Corporate Operations, Payroll will be responsible for sending these files to Records Management, the HR Advice and Support Teams will need to advise Corporate Operations, Payroll of any variations to the normal 7 year time-scale e.g. where personal files are to be kept for 25 years, or where disciplinary information is to be kept indefinitely so that it, in turn, can advise Records Management accordingly.

7. Updating of employment records

In order to ensure that employment records are accurate and up to date, the Council undertakes periodic file audits and data cleansing exercises in conjunction with the manager/employee for data held on the Oracle system.

8. Disclosing information about Workers to External Organisations

The Council is legally obliged to provide information to external organisations in certain defined circumstances, namely, the Inland Revenue, the Department of Work and Pensions and the Financial Services Authority.

Staff dealing with such requests should satisfy themselves as to the identity and authority of the person making the request, for example, obtaining the request in writing or telephoning/e-mailing back to a known number/address. Also, no more information than is necessary to satisfy the request should be disclosed.

9. Accessing Employment Data

As noted above, any employee, or ex-employee has the right to request, and receive a copy of all the employment information held on them, unless the information is covered by an exemption or restriction, or the effort involved in retrieving the information is disproportionate to the request.

Even where the effort involved in providing a copy of the information would be disproportionate to the request in terms of time, cost and difficulty (this to be balanced against the impact to the employee/former

employee of not providing the information), access to the record must still be given. The employee/former employee would be asked to highlight what records they want to access. As noted above (see also paragraph. 10.3), some information is exempt from access. Therefore each file must be checked before access is given. Particular care must be taken in respect of information about third parties. Where there is any doubt, advice should be sought from the IS information Management and Governance team or the HR Advice & Support Team.

In terms of access to e-mails, any e-mail which is about the particular worker must be provided. A realistic judgement will need to be made by the HR consultant dealing with the request and the employee's line manager (or former line manager) about which mail boxes are likely to contain e-mails about that worker in order that an appropriate search can be conducted. This is most likely to be the mailbox of the line manager, but if the worker provides information to the effect that other mailboxes are likely to contain information about them, then this should also be taken into account when conducting the search. The search should be coordinated by the HR consultant dealing with the request, in liaison with ISIS and the relevant line manager.

All requests for access to personal information must be in writing. Sufficient information must be provided to enable the information to be identified e.g. a person called John Smith may need to provide a middle name, date of birth and address to identify unique records. If further information is required to help locate the information e.g., date of leaving employment, then this can be requested and the timescale for providing the information will commence from the date of receipt of the clarifying information.
The HR Advice & Support team will ensure that the Access to Records team, located in SCF, are notified of all Data Subject Access requests which will be recorded on a corporate database. These will then be managed by the HR Advice & Support team who will record, collate, liaise with functions and prepare responses within 40 calendar days. The HR Advice & Support team will then inform the Access to Records team of the outcome of each request.
The same process will apply to medical records however, the request will be passed on to and responded to by the Occupational Health team.

In relation to data subject access requests relating to recruitment please contact the Working for Essex team who will record and produce responses for these requests.
For full guidance on handling requests for personal information please follow the attached link (insert link).

9.1 Current/former employees

Requests for access to personal information should be made in writing, using the data subject application form (Appendix 2) if applicable, to the Access to Records Team. The Access to Records is part of the Information Management and Governance team who will log the request and pass on to the relevant team/function for processing. Such requests should be processed by the relevant team as soon as possible, but no later than 40 calendar days following receipt.
In order to progress a written request for information disclosure, the HR advisor will need to:

- liaise with the Information Intelligence unit/payroll to obtain a copy of the basic employment record/details;
- liaise with the employee's line manager to identify any manual information held by the manager and also any e-mails about the individual;
- liaise with Payroll to obtain an employee's personal file;

- access, where relevant, recruitment documentation for interview notes etc;
- liaise with the Pensions and Payroll for relevant information, where appropriate.

Copies of all of the information listed in paragraph 3 above should be provided to the employee, unless agreement is reached with the employee that they do not wish to have access to certain records e.g. payroll or pensions records, held on them.

10. Information which does not have to be disclosed

10.1 Information not covered by the Act

Information of a more general or anonymous nature is not covered by the Act, for example, analyses of workforce information where individuals are not named or cannot be identified. This could include, for example, a report on the results of 'exit' interviews where all responses are anonymised.

10.2 Circumstances in which information should not be disclosed

Personal data does not have to be disclosed to the employee/former employee in certain, limited circumstances, including:

- to prevent or detect crime;
- to assess or collect tax;
- when the data relates to the physical health or mental state or condition of the individual (see below);
- where the data is protected by legal professional privilege.

10.3 Exempt Information – i.e. data which does not have to be disclosed to the worker under the Act

This is as follows:

- Confidential employment references. Under the DPA, employers do not have to provide employees with copies of confidential references written about them. However, as the Council operates an open reference policy employees are generally entitled to see any references written about them by the Council. Reference request letters to other employers refer to the fact the Council operates an 'open' reference policy and will be shown to the employee, on request.
- Employees do, however, have a right to request a copy of the reference from the recipient.
- Information relating to the physical or mental health of the data subject, without the opinion of the Council's Occupational Health Physician or unless the manager is satisfied that the data subject is already in receipt or knowledge of this information.
- Management forecasting and planning information to the extent that disclosure would prejudice the business e.g. information relating to potential redundancy situations.
- Information relating to negotiations with the individual, to the extent that disclosure would prejudice the negotiations e.g. if disclosed, the information would give away the 'fall back' position.
- Information relating to a third party. Where another individual is named in documentation relating to the individual requesting access to the information, the following steps should be taken:
    i. obtain the consent of that individual before releasing the information (if the 3rd party is contactable).
    ii. if consent is withheld, consider whether the information can be edited so as not to reveal the identity of the 3rd party.
    iii. if this is not possible, weigh up whether on balance the worker's right to know about the

information outweighs the right to privacy of the 3rd party.

11. Conclusion

Any individual seeking information or advice relating to data protection should raise the matter in the first instance with the IS Information Management and Governance on 033301 39824.

More information and help

Associated documents

Guides

- Guide 1 – Retention periods for employment information
- Guide 2 - Information Commission Code of Practice on Records Management
- Guide 4 – Personal files
- Guide 5 – Guidance to personal file management

Policies

- Employment of Ex-Offenders guidance
- Our Policy on Information Security and Communication
- Recruitment
- TUPE
- Subject Access Requests

Forms

- Subject Access Request form

Contact for more information

HR Advice and Support
Tel: 01245 430111 (Ednet 20111)
Email:
HRadviceandsupport@essex.gov.uk

Last updated: 19 June 2014
Changes made: Updates to team names for IS and removal of CSA.

Previous changes: Jan 14
Changes made: Team name change amendments

This document is issued by
Essex County Council, Human Resources.
You can contact us in the following ways:

By post:
Advice and Support, Human Resources,
County Hall, Chelmsford Essex CM1 1YS

By telephone:
03330 134 300

By email:
hradviceandsupport@essex.gov.uk

Read our online magazine at **essex.gov.uk/ew**

Follow us on **Essex_CC**

Find us on **facebook.com/essexcountycouncil**

The information contained in this document can be made available in alternative formats, on request.

DS09 1781

recycle for Essex

Essex County Council