Employee Privacy Policy & Statement

2018 - 2020

CYNGOR Sir y Fflint
Flintshire
COUNTY COUNCIL

Contents

Policy Scope and Context

In order to comply with its contractual, statutory, and management obligations and responsibilities, the Council is required to process personal data relating to its employees, including 'sensitive' personal data, as defined in the Data Protection Act 1998 (the "Act") which includes information relating to health, racial or ethnic origin, sexual orientation, and criminal convictions. All such data will be processed in accordance with the provisions of the Act and the Council Policy on Data Protection as amended from time to time.

We will work closely with individuals and other third parties to ensure that legislation and policy dealing with data protection in the human resources context strikes a workable balance between the legitimate interests of the Council as the employer, and our prospective, current and former employees.

We have established systems in place to protect individual's employment-related personal data. Our codes of conduct/policies protect employee data while allowing us to utilise processes designed to make our businesses more efficient and effective in managing and supporting our workforce. In protecting our workforce personal data we will not allow the misuse of individual's data and we shall protect our legitimate interests as an employer, and the vital interests and freedoms of our workforce.

All personal data relating to County Council personnel shall be:

- obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the employee concerned;
- processed within the strict terms of the law, including but not limited to the Data Protection Act 1998, and any associated rules, regulations, statutory provisions, extensions or re-enactments thereof and where possible, in line with any current guidance and other publications of the Information Commissioner;
- relevant for the purposes for which it is to be used;
- accurate, complete and up to date;
- kept for no longer than is necessary for its declared purpose;
- held in the full knowledge of the individual employee (except in cases specifically excluded under the Data Protection Act 1998);
- protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data;

Contractual responsibilities

The Council's contractual responsibilities include those arising from the contract of employment. The data processed to meet contractual responsibilities includes, but is not limited to, data relating to: payroll; bank account; postal address; sickness pay; maternity pay; leave; pension; and emergency contacts.

Statutory responsibilities

The Council's statutory responsibilities are those imposed on the Council by legislation. The data processed to meet statutory responsibilities includes, but is not limited to, data relating to: income tax; national insurance; statutory sickness pay; statutory maternity pay; family leave; work permits; and equal opportunities monitoring.

Management responsibilities

The Council's management responsibilities are those necessary for the organisational functioning of the Council. The data processed to meet management responsibilities includes, but is not limited to, data relating to: recruitment and employment; training and development; teaching; research; absence; disciplinary matters; health and safety; security, including Council-operated CCTV; e-mail address and telephone number; ID cards; and criminal convictions.

Sensitive personal data

The Act defines 'sensitive personal data' as information about racial or ethnic origin; political opinions; religious beliefs or other similar beliefs; trade union membership; physical or mental health; sexual life; and criminal allegations, proceedings or convictions. In certain limited circumstances, the Act permits the Council to collect and process sensitive personal data without requiring the explicit consent of the employee.

The following categories of information are subject to statutory restriction and will only be held on file for specific, legitimate purposes.

(a) *Racial or ethnic origin*
This will only be recorded on personnel files, with the express permission of each employee concerned, strictly for statistical purposes in connection with "ethnic monitoring'. – i.e. to identify and keep under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained.

(b) *Religious or philosophical beliefs*
This will only be held on file with the express permission of each employee.

(c) *Trade Union Membership*
This will only be held on file, with the express permission of each employee concerned, for the purposes of collecting union subscriptions by the County Council or associated employers.

(d) *The processing of data concerning gender, sexual orientation and gender re-assignment*

This will only be held with the express permission of the employee or in the case of gender where it is necessary to meet specific employment regulations or duties.

(e) *The processing of data concerning health*

Only data relating to:
(i) occupational health;
(ii) sickness absence records;
(iii) the chronic illness of a specific employee in circumstances which may affect their ability to perform all aspects of the normal work; and
(iv) data to comply with the Equality Act (2010)

Data relating to iii) and iv) above will be collected and retained only with the express permission of the individual employees concerned.

We recognise the rights of employees under the Rehabilitation of Offenders Act 1974 and any associated Orders of the Secretary of State, other rules, regulations, or statutory provisions and will maintain any conviction records (Data Barring Service Checks) on file for only those periods which are permissible under the Act. This will be in line with our entitlement under Schedule 3(2),(1) of the 1998 Data Protection Act.

Under Section 8 of the Asylum and Immigration Act of 1996 we are entitled to request, and hold copies of, documents specified within the Act for all new, and prospective, employees entering (or applying for) employment after 31 January 1997. This will be carried out without prejudice to employees' (and prospective employees') rights under the Race Relations Act 1976.

We reserve the right to 'back up' data files and hold secure multiple copies of personal data relating to specific employees in order to protect our interests in the event of data loss.

Disclosure of personal data to other bodies

For the performance of the employment contract, the Council is required to transfer an employee's personal data to third parties, for example, to pension providers and HM Revenue & Customs.

In order to fulfil its statutory responsibilities, the Council is required to provide some of an employee's personal data to government departments or agencies e.g. provision of salary and tax data to HM Revenue & Customs.

Keeping personal data up-to-date

The Act requires the Council to take reasonable steps to ensure that any personal data it processes is accurate and up-to-date. It is the responsibility of the individual

employee to inform the Council of any changes to the personal data that they have supplied to it during the course of their employment.

Requesting information

Under the Act, it is possible for individuals to request access to any of their personal data held by the Council, subject to certain restrictions. A request for disclosure of such information is called a subject access request. Any such requests should be addressed to the Council's Information Governance Team which can be done via the Council's website (http://www.flintshire.gov.uk/en/Resident/Data-Protection-and-Freedom-of-Information/Data-Protection.aspx)

Restriction of Access to Personnel Data

We may place all or part of our files onto secure computer networks and restrict access to personnel data. When implemented, access to individual employee data will only be granted to the following data users and only for specific and legitimate purposes:

- Individuals employed in the Human Resources Department (including Payroll);
- An employee's Head of Department/Executive/line manager;
- Individuals employed in the Pensions section of the Finance Department;
- Any specified and contracted third party (acting under the direction of the Data Controller, or his/her representative) used to process internal corporate data - providing secure processing facilities and data access in line with statutory provisions and the requirements of the County Council.

Retention

Application forms, interview records and references for unsuccessful internal and external candidates should be kept for a period of six months following the interview. Retention beyond this period would require demonstration of a clear business need by the Council and consent obtained from the individual. This applies to all manual files including any notes taken by anyone at interviews as well as computerised files.

There are a number of statutory minimum retention periods required by law within England and Wales. The specific retention periods for all employee related records are detailed in the Human Resources and Organisational Development Retention Schedule a copy of which can be found on the employment pages of the Infonet.

The Right to Object

An employee is entitled at any time, by notice in writing to the Council to request us to cease, within a reasonable time, from processing any personal data because it is causing or likely to cause, substantial damage or distress to themselves or another

individual. The reasons for this request must be clearly stated and specified at the time. We as the Data Controller will respond within twenty one days stating whether it intends or has complied as the reasons why the notice is unjustified and the extent to which it intends to comply (if at all).